Cyber Resilience Review (CRR): Self-Assessment Package

February 2014

Homeland Security

Organization Information

Facilitator:
    Name

    Phone

    Email

Date of Cyber Resilience Review   *(Please use popup calendar)*

Name of Organization/Business Unit

Sector

Critical Service

Physical Location:
    City

    State   Alabama

Critical Service Point of Contact:
    Name

    Phone

    Email

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.

Goal 1 – Services are identified and prioritized.

	Yes	Incomplete	No	
1. Is the organizations mission, vision, values and purpose, including the organizations place in critical infrastructure, identified and communicated? [EF:SG1.SP1]	☐	☐	☐	[c]
2. Are the organization's mission objectives and activities prioritized? [EF:SG1.SP3]	☐	☐	☐	[c]
3. Are services identified? [SC:SG2.SP1]	☐	☐	☐	[c]
4. Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	☐	☐	☐	[c]

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

	Yes	Incomplete	No	
1. Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]				
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]
2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]				
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]
3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]				
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]
4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]				
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

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

	Yes	Incomplete	No

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

	Yes	Incomplete	No	
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

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

	Yes	Incomplete	No	
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

Goal 4 – The asset inventory is managed.

	Yes	Incomplete	No

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

	Yes	Incomplete	No	
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

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

	Yes	Incomplete	No	
People	☐	☐	☐	[c]
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

Goal 5 – Access to assets is managed.

	Yes	Incomplete	No

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

	Yes	Incomplete	No	
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

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

	Yes	Incomplete	No	
Information	☐	☐	☐	[c]
Technology	☐	☐	☐	[c]
Facilities	☐	☐	☐	[c]

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

Information	☐	☐	☐ C
Technology	☐	☐	☐ C
Facilities	☐	☐	☐ C

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

Information	☐	☐	☐ C
Technology	☐	☐	☐ C
Facilities	☐	☐	☐ C

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

	Yes	Incomplete	No	
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] ⓖ	☐	☐	☐	C
2. Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2] ⓖ	☐	☐	☐	C
3. Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2] ⓖ	☐	☐	☐	C
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] ⓖ	☐	☐	☐	C
5. Are high-value information assets backed-up and retained? [KIM:SG6.SP1] ⓖ	☐	☐	☐	C
6. Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3] ⓖ	☐	☐	☐	C
7. Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3] ⓖ	☐	☐	☐	C

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

	Yes	Incomplete	No	
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] ⓖ	☐	☐	☐	C
2. Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1] ⓖ	☐	☐	☐	C
3. Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2] ⓖ	☐	☐	☐	C

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing asset management activities?	☐	☐	☐	c
	2. Is there a documented policy for asset management?	☐	☐	☐	c
	3. Have stakeholders for asset management activities been identified and made aware of their roles?	☐	☐	☐	c
	4. Have asset management standards and guidelines been identified and implemented?	☐	☐	☐	c

		Yes	Incomplete	No	
MIL3-Managed	1. Is there management oversight of the performance of the asset management activities?	☐	☐	☐	c
	2. Have qualified staff been assigned to perform asset management activities as planned?	☐	☐	☐	c
	3. Is there adequate funding to perform asset management activities as planned?	☐	☐	☐	c
	4. Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?	☐	☐	☐	c

		Yes	Incomplete	No	
MIL4-Measured	1. Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?	☐	☐	☐	c
	2. Are asset management activities periodically reviewed to ensure they are adhering to the plan?	☐	☐	☐	c
	3. Is higher-level management aware of issues related to the performance of asset management?	☐	☐	☐	c

		Yes	Incomplete	No	
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?	☐	☐	☐	c
	2. Are improvements to asset management activities documented and shared across the organization?	☐	☐	☐	c

Other Observations – Asset Management

2   Controls Management

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

Goal 1 – Control objectives are established.

	Yes	Incomplete	No	
1. Have control objectives been established for assets required for delivery of the critical service? [CTRL:SG1.SP1] ⓖ				
People	☐	☐	☐	C
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
2. Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1] ⓖ	☐	☐	☐	C

Goal 2 – Controls are implemented.

	Yes	Incomplete	No	
1. Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1] ⓖ	☐	☐	☐	C

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

	Yes	Incomplete	No	
1. Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1] ⓖ				
People	☐	☐	☐	C
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
2. As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1] ⓖ	☐	☐	☐	C

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

	Yes	Incomplete	No	
1. Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1] ⓖ				
People	☐	☐	☐	C
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
2. As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1] ⓖ	☐	☐	☐	C

MIL2-Planned

	Yes	Incomplete	No	
1. Is there a plan for performing controls management activities? ⓖ	☐	☐	☐	c
2. Is there a documented policy for controls management? ⓖ	☐	☐	☐	c
3. Have stakeholders for controls management activities have been identified and made aware of their roles? ⓖ	☐	☐	☐	c
4. Have controls management standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	c

MIL3-Managed

	Yes	Incomplete	No	
1. Is there management oversight of the performance of the controls management activities? ⓖ	☐	☐	☐	c
2. Have qualified staff been assigned to perform controls management activities as planned? ⓖ	☐	☐	☐	c
3. Is there adequate funding to perform controls management activities as planned? ⓖ	☐	☐	☐	c
4. Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	c

MIL4-Measured

	Yes	Incomplete	No	
1. Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	c
2. Are controls management activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	c
3. Is higher-level management aware of issues related to the performance of controls management? ⓖ	☐	☐	☐	c

MIL5-Defined

	Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	c
2. Are improvements to controls management documented and shared across the organization? ⓖ	☐	☐	☐	c

Other Observations – Controls Management

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.

Goal 1 – The life cycle of assets is managed.

	Yes	Incomplete	No	
1. Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]				
Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c
2. Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]				
Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c
3. Is capacity management and planning performed for assets? [TM:SG5.SP3]	☐	☐	☐	c
4. Are change requests tracked to closure? [TM:SG4.SP3]	☐	☐	☐	c
5. Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	☐	☐	☐	c

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

	Yes	Incomplete	No	
1. Is configuration management performed for technology assets? [TM:SG4.SP2]	☐	☐	☐	c
2. Are techniques in use to detect changes to technology assets? [TM:SG4.SP3]	☐	☐	☐	c
3. Are modifications to technology assets reviewed? [TM:SG4.SP2; TM:SG4.SP3]	☐	☐	☐	c
4. Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1]	☐	☐	☐	c
5. Is the integrity of information assets monitored? [KIM:SG5.SP3]	☐	☐	☐	c
6. Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2; TM:SG4.SP3]	☐	☐	☐	c
7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	☐	☐	☐	c
8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	☐	☐	☐	c

Goal 3 – Asset configuration baselines are established.

	Yes	Incomplete	No	
1. Do technology assets have configuration baselines? [TM:SG4.SP2]	☐	☐	☐	c
2. Is approval obtained for proposed changes to baselines? [TM:SG4.SP3]	☐	☐	☐	c

MIL2-Planned

	Yes	Incomplete	No	
1. Is there a documented plan for performing change management activities?	☐	☐	☐	c
2. Is there a documented policy for change management?	☐	☐	☐	c
3. Have stakeholders for change management activities been identified and made aware of their roles?	☐	☐	☐	c
4. Have change management standards and guidelines been identified and implemented?	☐	☐	☐	c

MIL3-Managed

	Yes	Incomplete	No	
1. Is there management oversight of the performance of the change management activities?	☐	☐	☐	c
2. Have qualified staff been assigned to perform change management activities as planned?	☐	☐	☐	c
3. Is there adequate funding to perform change management activities as planned?	☐	☐	☐	c
4. Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?	☐	☐	☐	c

MIL4-Measured

	Yes	Incomplete	No	
1. Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?	☐	☐	☐	c
2. Are change management activities periodically reviewed to ensure they are adhering to the plan?	☐	☐	☐	c
3. Is higher-level management aware of issues related to the performance of change management?	☐	☐	☐	c

MIL5-Defined

	Yes	Incomplete	No	
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?	☐	☐	☐	c
2. Are improvements to change management documented and shared across the organization?	☐	☐	☐	c

Other Observations – Configuration and Change Management

4 Vulnerability Management

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

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

	Yes	Incomplete	No	
1. Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2] ⓖ				
People	☐	☐	☐	C
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2] ⓖ				
People	☐	☐	☐	C
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C

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

	Yes	Incomplete	No	
1. Have sources of vulnerability information been identified? [VAR: SG2.SP1] ⓖ				
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
2. Is the information from these sources kept current? [VAR: SG2.SP1] ⓖ				
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C
3. Are vulnerabilities being actively discovered? [VAR: SG2.SP2] ⓖ				
Information	☐	☐	☐	C
Technology	☐	☐	☐	C
Facilities	☐	☐	☐	C

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

Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c

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

Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c

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

Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c

Goal 3 – Exposure to identified vulnerabilities is managed.

	Yes	Incomplete	No	
1. Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1] ⓖ	☐	☐	☐	c
2. Is the effectiveness of vulnerability mitigation reviewed? [VAR: SG3.SP1] ⓖ	☐	☐	☐	c
3. Is the status of unresolved vulnerabilities monitored? [VAR: SG3.SP1] ⓖ	☐	☐	☐	c

Goal 4 – The root causes of vulnerabilities are addressed.

	Yes	Incomplete	No	
1. Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR: SG4.SP1] ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing vulnerability management activities? ⓖ	☐	☐	☐	[c]
	2. Is there a documented policy for vulnerability management? ⓖ	☐	☐	☐	[c]
	3. Have stakeholders for vulnerability management activities been identified and made aware of their roles? ⓖ	☐	☐	☐	[c]
	4. Have vulnerability management standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	[c]

		Yes	Incomplete	No	
MIL3-Managed	1. Is there management oversight of the performance of the vulnerability management activities? ⓖ	☐	☐	☐	[c]
	2. Have qualified staff been assigned to perform vulnerability management activities as planned? ⓖ	☐	☐	☐	[c]
	3. Is there adequate funding to perform vulnerability management activities as planned? ⓖ	☐	☐	☐	[c]
	4. Are risks related to the performance of planned vulnerability management activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	[c]

		Yes	Incomplete	No	
MIL4-Measured	1. Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	[c]
	2. Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	[c]
	3. Is higher-level management aware of issues related to the performance of vulnerability management? ⓖ	☐	☐	☐	[c]

		Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	[c]
	2. Are improvements to vulnerability management activities documented and shared across the organization? ⓖ	☐	☐	☐	[c]

Other Observations – Vulnerability Management

5 Incident Management

The purpose of Incident Management is to establish processes to identify and analyze events, detect incidents, and determine an organizational response.

Goal 1 – A process for identifying, analyzing, responding to, and learning from incidents is established.

	Yes	Incomplete	No	
1. Does the organization have a plan for managing incidents? [IMC:SG1.SP1] ⓖ	☐	☐	☐	c
2. Is the incident management plan reviewed and updated? [IMC:SG1.SP1] ⓖ	☐	☐	☐	c
3. Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2] ⓖ	☐	☐	☐	c
4. Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2] ⓖ	☐	☐	☐	c

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

	Yes	Incomplete	No	
1. Are events detected and reported? [IMC:SG2.SP1] ⓖ	☐	☐	☐	c
2. Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2] ⓖ	☐	☐	☐	c
3. Are events categorized? [IMC:SG2.SP4] ⓖ	☐	☐	☐	c
4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4] ⓖ	☐	☐	☐	c
5. Are events prioritized? [IMC:SG2.SP4] ⓖ	☐	☐	☐	c
6. Is the status of events tracked? [IMC:SG2.SP4] ⓖ	☐	☐	☐	c
7. Are events managed to resolution? [IMC:SG2.SP4] ⓖ	☐	☐	☐	c
8. Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3] ⓖ	☐	☐	☐	c
9. Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3] ⓖ	☐	☐	☐	c

Goal 3 – Incidents are declared and analyzed.

	Yes	Incomplete	No	
1. Are incidents declared? [IMC:SG3.SP1] ⓖ	☐	☐	☐	c
2. Have criteria for the declaration of an incident been established? [IMC.SG3.SP1] ⓖ	☐	☐	☐	c
3. Are incidents analyzed to determine a response? [IMC.SG3.SP2] ⓖ	☐	☐	☐	c

Goal 4 – A process for responding to and recovering from incidents is established.

	Yes	Incomplete	No	
1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1] ⓖ	☐	☐	☐	[c]
2. Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2] ⓖ	☐	☐	☐	[c]
3. Are incident status and response communicated to affected parties? [IMC:SG4.SP3] ⓖ	☐	☐	☐	[c]
4. Are incidents tracked to resolution? [IMC:SG4.SP4] ⓖ	☐	☐	☐	[c]

Goal 5 – Post-incident lessons learned are translated into improvement strategies.

	Yes	Incomplete	No	
1. Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1] ⓖ	☐	☐	☐	[c]
2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2] ⓖ	☐	☐	☐	[c]
3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3] ⓖ	☐	☐	☐	[c]

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing incident management activities? ⓖ	☐	☐	☐	c
	2. Is there a documented policy for incident management? ⓖ	☐	☐	☐	c
	3. Have stakeholders for incident management activities been identified and made aware of their roles? ⓖ	☐	☐	☐	c
	4. Have incident management standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL3-Managed	1. Is there management oversight of the performance of the incident management activities? ⓖ	☐	☐	☐	c
	2. Have qualified staff been assigned to perform incident management activities as planned? ⓖ	☐	☐	☐	c
	3. Is there adequate funding to perform incident management activities as planned? ⓖ	☐	☐	☐	c
	4. Are risks related to the performance of planned incident management activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL4-Measured	1. Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	c
	2. Are incident management activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	c
	3. Is higher-level management aware of issues related to the performance of incident management? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	c
	2. Are improvements to incident management activities documented and shared across the organization? ⓖ	☐	☐	☐	c

Other Observations – Incident Management

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.

Goal 1 – Service continuity plans for high-value services are developed.

	Yes	Incomplete	No	
1. Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2]				
People	☐	☐	☐	c
Information	☐	☐	☐	c
Technology	☐	☐	☐	c
Facilities	☐	☐	☐	c
2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	☐	☐	☐	c
3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	☐	☐	☐	c
4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	☐	☐	☐	c
5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	☐	☐	☐	c
6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	☐	☐	☐	c

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

	Yes	Incomplete	No	
1. Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	☐	☐	☐	c

Goal 3 - Service continuity plans are tested to ensure they meet their stated objectives.

	Yes	Incomplete	No	
1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	☐	☐	☐	c
2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	☐	☐	☐	c
3. Are service continuity plans tested? [SC:SG5.SP3]	☐	☐	☐	c
4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	☐	☐	☐	c
5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	☐	☐	☐	c

Goal 4 – Service continuity plans are executed and reviewed

	Yes	Incomplete	No	
1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1] ⓖ	☐	☐	☐	ⓒ
2. Is execution of service continuity plans reviewed? [SC:SG6.SP2] ⓖ	☐	☐	☐	ⓒ
3. Are improvements identified as result of executing service continuity plans? (SC:SG7.SP2) ⓖ	☐	☐	☐	ⓒ

MIL2-Planned

	Yes	Incomplete	No	
1. Is there a documented plan for performing service continuity activities? ⓖ	☐	☐	☐	ⓒ
2. Is there a documented policy for service continuity? ⓖ	☐	☐	☐	ⓒ
3. Have stakeholders for service continuity activities been identified and made aware of their roles? ⓖ	☐	☐	☐	ⓒ
4. Have service continuity standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	ⓒ

MIL3-Managed

	Yes	Incomplete	No	
1. Is there management oversight of the performance of the service continuity activities? ⓖ	☐	☐	☐	ⓒ
2. Have qualified staff been assigned to perform service continuity activities as planned? ⓖ	☐	☐	☐	ⓒ
3. Is there adequate funding to perform service continuity activities as planned? ⓖ	☐	☐	☐	ⓒ
4. Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	ⓒ

MIL4-Measured

	Yes	Incomplete	No	
1. Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	ⓒ
2. Are service continuity activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	ⓒ
3. Is higher-level management aware of issues related to the performance of service continuity? ⓖ	☐	☐	☐	ⓒ

MIL5-Defined

	Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	ⓒ
2. Are improvements to service continuity documented and shared across the organization? ⓖ	☐	☐	☐	ⓒ

Other Observations – Service Continuity Management

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.

Goal 1 – A strategy for identifying, analyzing, and mitigating risks is developed.

	Yes	Incomplete	No	
1. Have sources of risk that can affect operations been identified? [RISK: SG1.SP1]	☐	☐	☐	c
2. Have categories been established for risks? [RISK: SG1.SP1]	☐	☐	☐	c
3. Has a plan for managing operational risk been established? [RISK: SG1.SP2]	☐	☐	☐	c
4. Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]	☐	☐	☐	c

Goal 2 – Risk tolerances are identified, and the focus of risk management activities is established.

	Yes	Incomplete	No	
1. Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]	☐	☐	☐	c
2. Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]	☐	☐	☐	c
3. Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]	☐	☐	☐	c
4. Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]	☐	☐	☐	c

Goal 3 – Risks are identified.

	Yes	Incomplete	No	
1. Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]	☐	☐	☐	c

Goal 4 – Risks are analyzed and assigned a disposition.

	Yes	Incomplete	No	
1. Are risks analyzed to determine potential impact to the critical service? [RISK: SG4.SP1]	☐	☐	☐	c
2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]	☐	☐	☐	c

Goal 5 – Risks to assets and services are mitigated and controlled.

	Yes	Incomplete	No	
1. Are plans developed for risks that the organization decides to mitigate? [RISK: SG5.SP1]	☐	☐	☐	c
2. Are identified risks tracked to closure? [RISK: SG5.SP2]	☐	☐	☐	c

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing risk management activities? ⓖ	☐	☐	☐	c
	2. Is there a documented policy for risk management? ⓖ	☐	☐	☐	c
	3. Have stakeholders for risk management activities have identified and made aware of their roles? ⓖ	☐	☐	☐	c
	4. Have risk management activities standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL3-Managed	1. Is there management oversight of the performance of the risk management activities? ⓖ	☐	☐	☐	c
	2. Have qualified staff been assigned to perform risk management activities as planned? ⓖ	☐	☐	☐	c
	3. Is there adequate funding to perform risk management activities as planned? ⓖ	☐	☐	☐	c
	4. Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL4-Measured	1. Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	c
	2. Are risk management activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	c
	3. Is higher-level management aware of issues related to the performance of risk management? ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	c
	2. Are improvements to risk management documented and shared across the organization? ⓖ	☐	☐	☐	c

Other Observations – Risk Management

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.

Goal 1 – External dependencies are identified and prioritized to ensure sustained operation of high-value services.

	Yes	Incomplete	No	
1. Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1] ⓖ	☐	☐	☐	⊏c⊐
2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1] ⓖ	☐	☐	☐	⊏c⊐
3. Are external dependencies prioritized? [EXD:SG1.SP2] ⓖ	☐	☐	☐	⊏c⊐

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

	Yes	Incomplete	No	
1. Are risks due to external dependencies identified and managed? [EXD:SG2.SP1] ⓖ	☐	☐	☐	⊏c⊐

Goal 3 – Relationships with external entities are formally established and maintained.

	Yes	Incomplete	No	
1. Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2] ⓖ	☐	☐	☐	⊏c⊐
2. Are these requirements reviewed and updated? [EXD:SG3.SP2] ⓖ	☐	☐	☐	⊏c⊐
3. Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3] ⓖ	☐	☐	☐	⊏c⊐
4. Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4] ⓖ	☐	☐	☐	⊏c⊐

Goal 4 – Performance of external entities is managed.

	Yes	Incomplete	No	
1. Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1] ⓖ	☐	☐	☐	⊏c⊐
2. Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1] ⓖ	☐	☐	☐	⊏c⊐
3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2] ⓖ	☐	☐	☐	⊏c⊐
4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2] ⓖ	☐	☐	☐	⊏c⊐

Goal 5 – Dependencies on public services and infrastructure service providers are identified.

	Yes	Incomplete	No	
1. Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3] ⓖ	☐	☐	☐	C
2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4] ⓖ	☐	☐	☐	C

MIL2-Planned

	Yes	Incomplete	No	
1. Is there a documented plan for performing external dependency management activities? ⓖ	☐	☐	☐	C
2. Is there a documented policy for external dependency management? ⓖ	☐	☐	☐	C
3. Have stakeholders for external dependency management activities been identified and made aware of their roles? ⓖ	☐	☐	☐	C
4. Have external dependency management activities standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	C

MIL3-Managed

	Yes	Incomplete	No	
1. Is there management oversight of the performance of the external dependency management activities? ⓖ	☐	☐	☐	C
2. Have qualified staff been assigned to perform external dependency management activities as planned? ⓖ	☐	☐	☐	C
3. Is there adequate funding to perform external dependency management activities as planned? ⓖ	☐	☐	☐	C
4. Are risks related to the performance of external dependency management activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	C

MIL4-Measured

	Yes	Incomplete	No	
1. Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	C
2. Are external dependency management activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	C
3. Is higher-level management aware of issues related to external dependency management? ⓖ	☐	☐	☐	C

MIL5-Defined

	Yes	Incomplete	No	
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? ⓖ	☐	☐	☐	C
2. Are improvements to external dependency management documented and shared across the organization? ⓖ	☐	☐	☐	C

Other Observations – External Dependencies Management

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.

Goal 1 – Cyber security awareness and training programs are established.

	Yes	Incomplete	No	
1. Have cyber security awareness needs been identified for the critical service? [OTA:SG1.SP1]	☐	☐	☐	c
2. Have required skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	☐	☐	☐	c
3. Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]	☐	☐	☐	c
4. Have training needs been identified? [OTA:SG3.SP1]	☐	☐	☐	c

Goal 2 – Awareness and training activities are conducted.

	Yes	Incomplete	No	
1. Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]	☐	☐	☐	c
2. Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	☐	☐	☐	c
3. Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	☐	☐	☐	c
4. Are awareness and training activities revised as needed? [OTA:SG1.SP3 and OTA:SG3.SP3]	☐	☐	☐	c

			Yes	Incomplete	No	
MIL2-Planned	1.	Is there a documented plan for performing training activities? ⓖ	☐	☐	☐	⊏
	2.	Is there a documented policy for training? ⓖ	☐	☐	☐	⊏
	3.	Have stakeholders for training activities been identified and made aware of their roles? ⓖ	☐	☐	☐	⊏
	4.	Have training standards and guidelines been identified and implemented? ⓖ	☐	☐	☐	⊏

			Yes	Incomplete	No	
MIL3-Managed	1.	Is there management oversight of the performance of the training activities? ⓖ	☐	☐	☐	⊏
	2.	Have qualified staff been assigned to perform training activities as planned? ⓖ	☐	☐	☐	⊏
	3.	Is there adequate funding to perform training activities as planned? ⓖ	☐	☐	☐	⊏
	4.	Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled? ⓖ	☐	☐	☐	⊏

			Yes	Incomplete	No	
MIL4-Measured	1.	Are training activities periodically reviewed and measured to ensure they are effective and producing intended results? ⓖ	☐	☐	☐	⊏
	2.	Are training activities periodically reviewed to ensure they are adhering to the plan? ⓖ	☐	☐	☐	⊏
	3.	Is higher-level management aware of issues related to the performance of training? ⓖ	☐	☐	☐	⊏

			Yes	Incomplete	No	
MIL5-Defined	1.	Has the organization adopted a standard definition of the training activities from which operating units can derive practices that fit their unique operating circumstances? ⓖ	☐	☐	☐	⊏
	2.	Are improvements to training documented and shared across the organization? ⓖ	☐	☐	☐	⊏

Other Observations – Training and Awareness

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.

Goal 1 – Threat monitoring is performed.

	Yes	Incomplete	No	
1. Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]	☐	☐	☐	c
2. Have threat monitoring procedures been implemented? [MON:SG2.SP2]	☐	☐	☐	c
3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3]	☐	☐	☐	c

Goal 2 – The requirements for communicating threat information are established.

	Yes	Incomplete	No	
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]	☐	☐	☐	c
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]	☐	☐	☐	c

Goal 3 – Threat information is communicated.

	Yes	Incomplete	No	
1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]	☐	☐	☐	c
2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	☐	☐	☐	c
3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	☐	☐	☐	c

		Yes	Incomplete	No	
MIL2-Planned	1. Is there a documented plan for performing situational awareness activities? Ⓖ	☐	☐	☐	c
	2. Is there a documented policy for situational awareness? Ⓖ	☐	☐	☐	c
	3. Have stakeholders for situational awareness activities been identified and made aware of their roles? Ⓖ	☐	☐	☐	c
	4. Have situational awareness standards and guidelines been identified and implemented? Ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL3-Managed	1. Is there management oversight of the performance of situational awareness activities? Ⓖ	☐	☐	☐	c
	2. Have qualified staff been assigned to perform situational awareness activities as planned? Ⓖ	☐	☐	☐	c
	3. Is there adequate funding to perform situational awareness activities as planned? Ⓖ	☐	☐	☐	c
	4. Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled? Ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
MIL4-Measured	1. Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results? Ⓖ	☐	☐	☐	c
	2. Are situational awareness activities periodically reviewed to ensure they are adhering to the plan? Ⓖ	☐	☐	☐	c
	3. Is higher-level management aware of issues related to situational awareness? Ⓖ	☐	☐	☐	c

		Yes	Incomplete	No	
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? Ⓖ	☐	☐	☐	c
	2. Are improvements to situational awareness activities documented and shared across the organization? Ⓖ	☐	☐	☐	c

Other Observations – Situational Awareness

PLEASE USE THE BUTTONS BELOW TO GENERATE AND PRINT THE REPORT

[Generate Report]   [Print Report]

CYBER RESILIENCE REVIEW

SELF-ASSESSMENT REPORT

FOR

Table of Contents

Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages and including damages based on any negligence of the United States Government or its contractors or subcontractors, arising out of, resulting from, or in any way connected with this report, whether or not based upon warranty, contract, tort, or otherwise, whether or not injury was sustained from, or arose out of the results of, or reliance upon the report.

The DHS does not endorse any commercial product or service, including the subject of the analysis in this report. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by DHS.

The display of the DHS official seal or other DHS visual identities on this report shall not be interpreted to provide the recipient organization authorization to use the official seal, insignia or other visual identities of the Department of Homeland Security. The DHS seal, insignia, or other visual identities shall not be used in any manner to imply endorsement of any commercial product or activity by DHS or the United States Government. Use of the DHS seal without proper authorization violates federal law (e.g., 18 U.S.C. §§ 506, 701, 1017), and is against DHS policies governing usage of its seal.

Cyber Resilience Review Report for

Introduction

On , conducted a Cyber Resilience Review (CRR) Self-Assessment. Answers to questions about cybersecurity practices were gathered from key stakeholders within and scored.

Overview and Scope of the CRR

The CRR consists of a one-day, structured facilitation and interview of key personnel. The primary goal of the CRR is to develop an understanding and qualitative measurement of essential cyber security capabilities. Personnel are asked to describe how these capabilities are institutionalized and managed, and how these capabilities are applied to support the organization during times of stress. The assessment questions asked participants to articulate evidence regarding both performances of cyber security practices as well as sustainment of those practices over time. Individual organizations are examined for specific capacities and capabilities in defining, managing, and measuring cyber security practices and behaviors, as described in categories. The categories examined are:

1   Asset Management
2   Controls Management
3   Configuration and Change Management
4   Vulnerability Management
5   Incident Management
6   Service Continuity Management
7   Risk Management
8   External Dependencies Management
9   Training and Awareness
10   Situational Awareness

The categories examined are derived from a larger security and business continuity framework known as the CERT® Resilience Management Model (CERT-RMM), which was developed by the CERT Program at Carnegie Mellon University's Software Engineering Institute.

About This Report

The CRR has a service orientation, meaning that one of the foundational principles of its design is the idea that an organization deploys its people, information, technology and facilities to support specific operational missions. During the CRR, this focus on services is how improves its understanding of the cyber security management of services that support critical infrastructure. This improved understanding helps the organization focus its efforts in improving cyber security management.

For this assessment, the critical infrastructure service is .

This report summarizes the assessment findings and provides your organization with options for consideration in each category. The options for consideration aim to provide general guidelines or activities as to how your organization can improve the organization's cyber security posture and preparedness. These options are not meant to fully represent all activities needed for a robust cyber security management program, but to provide initial guidance on how to incorporate various cyber security practices including CERT® Resilience Management Model (CERT-RMM), National Institute of Standard and Technology (NIST), and other cyber security standards.

Please note that guidance provided in this report includes National Institute of Standards and Technology (NIST) Special Publications. While the primary audience for these documents is United States Federal Civilian Agencies, NIST encourages the adoption of these guidelines by State, local, and tribal governments, as well as private sector organizations. Additionally, while the CRR bases its questions and options for consideration on CERT-RMM, the results do not constitute a formal "rating" and should not be interpreted as a formal appraisal of your organization against CERT-RMM. Detailed information about the RMM can be found at www.cert.org/resilience.   Options for Consideration appearing in italics have been derived from the Specific Goals (SG) and Specific Practices (SP) sections of the CERT-RMM.

Cyber Resilience Review Results

The CRR is an interview-based assessment. It is understood that participants often do not have complete knowledge of an organization's operations. Actual performance may vary from what is indicated in this report. Organizational performance is presented across several dimensions within the report. Scores are provided for individual Practices, Goals, and Domains.

Basic Rules

1. Practices are either performed (answer ="Yes"), incompletely performed (answer = "Incomplete"), or not performed (answer = "No")

2. A goal is achieved only if all practices are performed

3. A Domain is achieved at MIL-1 if all the Goals in the Domain are achieved

4. A Domain can be achieved at higher levels if the MIL questions for each level (MIL-2 through MIL-5) are answered.

Scoring Rubric

Step 1

Each Practice in a Domain is scored as the following:
- performed when the question is answered with a "Yes" (green)
- not performed when a question is answered with an "Incomplete" (yellow) or "No" (red) or "Not Answered" (grey)
- if "Not Answered" (grey) is shown, the question was left blank and is scored the same as a "No"

Step 2

Each Goal within the Domain is then scored as the following:
- achieved when all practices are performed (green)
- partially achieved when some practices are performed (yellow)
- not achieved when no practices are performed (red)

Step 3

Each Domain is assigned a MIL level based on the following:
- MIL-0 if only some of the goals are achieved
- MIL-1 if all of the goals are achieved
- MIL-2 if MIL-1 is achieved and all of the MIL-2 questions are answered YES
- MIL-3 if MIL-2 is achieved and all of the MIL-3 questions are answered YES
- MIL-4 if MIL-3 is achieved and all of the MIL-4 questions are answered YES
- MIL-5 if MIL-4 is achieved and all of the MIL-5 questions are answered YES

Maturity Indicator Levels

Maturity Indicator Levels (MIL) are assigned by Domain and represent a consolidated view of performance. CERT-RMM MILs describe attributes that would be indicative of mature capabilities as represented in the model's capability levels. However, they do not fully represent capability levels as defined because a capability level can only be assigned through a formal appraisal process, not as the result of using an assessment-based instrument.

MIL0   Incomplete

Indicates that Practices in the Domain are not being performed as measured by responses to the relevant CRR questions. If MIL0 is assigned, no further assessment of maturity indicator is performed.

MIL1   Performed

Indicates that all Practices in a Domain are being performed as measured by responses to the relevant CRR questions. MIL1 means that there is sufficient and substantial support for the existence of the practices.

MIL2   Planned

Indicates that all Practices in Domain are not only performed, but are supported by sufficient planning, stakeholders, and relevant standards and guidelines. A planned process/practice is
- established by the organization (Is the practice documented and communicable to all who need to know?)
- planned (Is the practice performed according to a documented plan?)
- supported by stakeholders (Are the stakeholders of the practice known and are they aware of the practice and their role in the practice?)
- supported by relevant standards and guidelines (Have the standards and guidelines that support the practice been identified and implemented?)

MIL3   Managed

Indicates that all Practices in a Domain are performed, planned, and have the basic infrastructure in place to support the process. A managed process/practice
- is governed by the organization (Is the practice supported by policy and is there appropriate oversight over the performance of the practice?)
- is appropriately staffed and funded (Are the staff and funds necessary to perform the practice as intended available?)
- is assigned to staff who are responsible and accountable for the performance of the practice (Have staff been assigned to perform the practice and are they responsible and accountable for the performance of the practice?)
- is performed by staff who are adequately trained to perform the practice (Are the staff who perform the practice adequately skilled and trained to perform the practice?)

- produces work products that are expected from performance of the practice and are placed under appropriate levels of configuration control (Does the practice produce artifacts and work products that are expected from performing the practice, and if so, are the configurations of these artifacts/work products managed?)

- is managed for risk (Are risks related to the performance of the practice identified, analyzed, disposed of, monitored, and controlled?)

MIL4   Measured

Indicates that all Practices in a Domain are performed, planned, managed, monitored, and controlled. A measured process/practice is

- periodically evaluated for effectiveness (Is the practice periodically reviewed to ensure that it is effective and producing intended results?)

- monitored and controlled (Are appropriate implementation and performance measures identified, applied, and analyzed?)

- objectively evaluated against its practice description and plan (Is the practice periodically evaluated to ensure that it adheres to the practice description and the plan for the practice?)

- periodically reviewed with higher-level management (Is higher-level management aware of any issues related to the performance of the practice?)
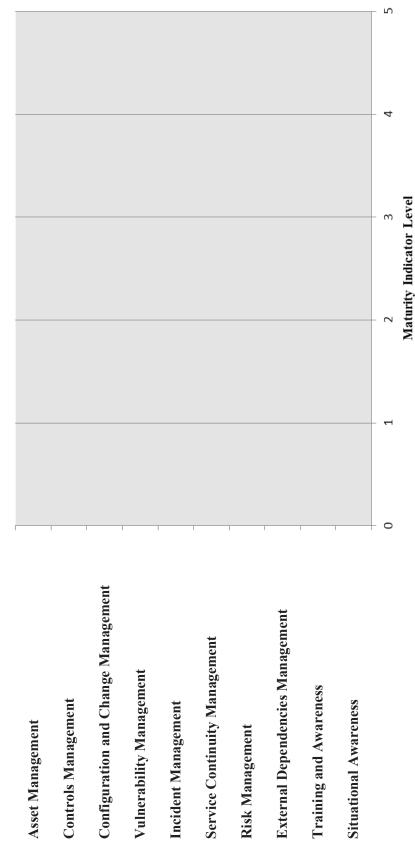
MIL5   Defined

Indicates that all Practices in a Domain are performed, planned, managed, monitored, controlled, and consistent across all internal[1] constituencies who have a vested interest in the performance of the practice. A defined process/practice ensures that the organization reaps the benefits of consistent performance of the practice across organizational units and that all organizational units can benefit from improvements realized in any organizational unit. At MIL5, a process/practice

- is defined by the organization and tailored by organizational units for their use (Is there an organization-sponsored definition of the practice from which organizational units can derive practices that fit their unique operating circumstances?)

- is supported by improvement information that is collected by and shared among organizational units for the overall benefit of the organization (Are practice improvements documented and shared across internal constituencies so that the organization as a whole reaps benefits from these improvements?)

[1] In this case, "internal" refers to constituencies over which the organization has direct managerial control.

Summary of Results

Maturity Indicator Level by Domain

Asset Management

Controls Management

Configuration and Change Management

Vulnerability Management

Incident Management

Service Continuity Management

Risk Management

External Dependencies Management

Training and Awareness

Situational Awareness

0 1 2 3 4 5

Maturity Indicator Level

Overview of CRR Results

	MIL-1							MIL-2				MIL-3				MIL-4			MIL-5	
1 Asset Management	G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
2 Controls Management	G1	G2	G3	G4				IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
3 Configuration and Change Management	G1	G2	G3					IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
4 Vulnerability Management	G1	G2	G3	G4				IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
5 Incident Management	G1	G2	G3	G4	G5			IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
6 Service Continuity Management	G1	G2	G3	G4				IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
7 Risk Management	G1	G2	G3	G4	G5			IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
8 External Dependencies Management	G1	G2	G3	G4	G5			IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
9 Training and Awareness	G1	G2						IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2
10 Situational Awareness	G1	G2	G3					IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

1   Asset Management

MIL-1								MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	L1	L2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

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]	
2.	Are the organization's mission objectives and activities prioritized? [EF:SG1.SP3]	
3.	Are services identified? [SC:SG2.SP1]	
4.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[EF:SG1.SP1]** Identify the organization's mission, vision, values, and purpose. From a resilience management perspective, the identification, comprehension, and communication of the organization's strategic objectives provides essential and necessary guidance and direction for the operational resilience management process. Effective operational resilience ensures that the organization can reach its strategic objectives. **Additional References:** NIST SP 800-53 Rev. 4 PM-8	
Q2	**CERT-RMM Reference** **[EF:SG1.SP3]** Prioritize and document the organizations strategic objectives. In order to appropriately scope the organization's operational resilience management process and corresponding operational resilience management activities, the high-value services of the organization that support the strategic objectives must be identified, prioritized, and communicated as a common target for success. Affinity analysis between the organization's strategic objectives and services is a means to help the organization prioritize services and to identify high-value services that must be made resilient. **Additional References:** NIST SP 800-53 Rev. 4 PM-11	

Q3	**CERT-RMM Reference** **[SC:SG2.SP1]** Identify the organization's high-value services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 15-18	
Q4	**CERT-RMM Reference** **[SC:SG2.SP1]** Prioritize and document the list of high-value services that must be provided if a disruption occurs. 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. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 16-18	
Goal 2 – Assets are inventoried, and authority and responsibility for these assets is established.		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	
	Information	
	Technology	
	Facilities	
2.	Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	
	People	
	Information	
	Technology	
	Facilities	
3.	Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	
	People	
	Information	
	Technology	
	Facilities	

4.	Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	
	People	
	Information	
	Technology	
	Facilities	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[ADM:SG1.SP1]** Identify and inventory high-value assets. An organization must be able to identify its high-value assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to services. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 2-3	
Q2	**CERT-RMM Reference** **[ADM:SG1.SP2]** Update the asset database with asset profile information. All information relevant to the asset (collected from the asset profile) should be contained with the asset in its entry in the asset database. Strategies to protect and sustain an asset may be documented as part of the asset profile.	
Q3	**CERT-RMM Reference** **[ADM:SG1.SP3]** Document and describe the owner of each asset on the asset profile. The organization should also, to the extent possible, identify relevant custodians for each high-value asset. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 19-21	
Q4	**CERT-RMM Reference** **[ADM:SG1.SP3]** Document and describe the physical location of the asset and the custodian of the asset. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems" Page 19-24	

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]	
People	
Information	
Technology	
Facilities	
2. Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	
People	
Information	
Technology	
Facilities	
Option(s) for Consideration:	
Q1 **CERT-RMM Reference** **[ADM:SG2.SP1]** Assign assets in the asset database to one or more services. The relationship between assets and the services they support must be understood in order to effectively develop, implement, and manage resilience strategies that support the accomplishment of the service's mission. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 21	
Q2 **CERT-RMM Reference** **[RRD:SG2.SP1]** Document confidentiality, integrity, and availability requirements for each service-related asset. The needs of the organization are satisfied by consistent and efficient performance of services. These services depend on the contributions and support of assets to meet their missions. Thus, the resilience of these assets is paramount to mission assurance. **Additional References** FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems, Page 2	

Goal 4 – The asset inventory is managed.	
1. Have change criteria been established for asset descriptions? [ADM:SG3.SP1]	
People	
Information	
Technology	
Facilities	
2. Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]	
People	
Information	
Technology	
Facilities	
Option(s) for Consideration:	
Q1 **CERT-RMM Reference** [ADM:SG3.SP1] Develop and document criteria for establishing when a change in asset inventory must be considered. Ensure that these criteria are commensurate with the organization's risk tolerances. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 21	
Q2 **CERT-RMM Reference** [ADM:SG3.SP2] Document the asset changes by updating asset profiles and the asset database. **Additional References** Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems", Page 26	
Goal 5 – Access to assets is managed.	
1. Is access to assets granted based on their protection requirements? [AM:SG1.SP1]	
Information	
Technology	
Facilities	
2. Are access requests reviewed and approved by the asset owner? [AM:SG1.SP1]	
Information	
Technology	
Facilities	

3.	Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3]	
	Information	
	Technology	
	Facilities	
4.	Are access privileges modified as a result of reviews? [AM:SG1.SP3]	
	Information	
	Technology	
	Facilities	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** [AM:SG1.SP1] Access privileges are assigned and approved by asset owners based on the role of the person, object, or entity that is requesting access. Asset owners are the persons or organizational units, internal or external to the organization, who have primary responsibility for the viability, productivity, and resilience of a high-value organizational asset. It is the owner's responsibility to ensure that requirements for protecting and sustaining assets are defined for assets under their control. In part, these requirements are satisfied by defining and assigning access privileges that are commensurate with the requirements. Therefore, the asset owner is responsible for granting and revoking access privileges to an identity based on the identity's role and the asset's resilience requirements. To be successful, asset owners must be aware of identities that need access to their assets and must evaluate the need with respect to business and resilience requirements before granting approval. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations", AC-1	
Q2	**CERT-RMM Reference** [AM:SG1.SP1] Access requests should be sponsored by an appropriate person in the organization (i.e., a supervisor or manager) and should be directly submitted to and approved by the owner of the assets (or their agents) to which access is being requested. Access requests should include proper justification for the request and should be approved by the sponsor of the request. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" AC-1	

Q3	**CERT-RMM Reference** **[AM:SG1.SP3]** The mismanagement of access privileges is a major source of potential risks and vulnerabilities to the organization. Because assets and the identity community that needs access to the assets are pervasive across the organization, and in some cases extend beyond the organization, the ability to ensure that only authorized identities have appropriate privileges is an ongoing challenge. The organization must establish responsibility for regular review of access privileges and a process for correcting inconsistencies. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" AC-2	
Q4	**CERT-RMM Reference** **[AM:SG1.SP3]** Asset owners should document any inconsistencies or misalignment in access privileges. Owners should identify privileges that are: • excessive • out of alignment with the identity's role or job responsibility • assigned but never approved by the asset owner • in violation of the asset's resilience requirements Owners should also identify identities that may have been provisioned with access privileges but are no longer considered as valid identities. A disposition for each inconsistency or misalignment should be documented, as well as the actions that need to be taken to correct these issues. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" AC-2	
Goal 6 – Information assets are prioritized 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]	
2	Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2]	
3	Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2]	
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]	
5	Are high-value information assets backed-up and retained ? [KIM:SG6.SP1]	
6	Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	
7	Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[KIM:SG1.SP2]** Assign sensitivity categorization levels to information assets. This practice typically occurs when the information asset is defined. The categorization level should be kept as part of the definition of the information asset in the asset inventory. **Additional References** FIPS Publication 200 "Minimum Security Requirements for Federal information and information Systems", Page 2	
Q2	**CERT-RMM Reference** **[KIM:SG2.SP2]** Establish and implement administrative controls for information assets. Administrative controls for protecting information assets include information security policies that govern the behavior of users, including policies for the proper sensitivity categorization of information assets. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 45-48	
Q3	**CERT-RMM Reference** **[KIM:SG1.SP2]** Establish policies for proper handling of information assets according to the sensitivity categorization scheme. Establish policies and procedures for proper labeling for each category of information asset. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" MP-3	
Q4	**CERT-RMM Reference** **[KIM:SG1.SP2]** Assign responsibility for the assignment of sensitivity categorization levels to information assets. All staff who handle information assets (including those who are external to the organization) should be trained in the organization's sensitivity categorization scheme and be authorized to assign a categorization level. Training should also be provided for proper handling of each category of information asset.	

Q5	**CERT-RMM Reference** **[KIM:SG6.SP1]** Develop information asset backup and retention procedures.Information asset backup and retention procedures should include: • standards for the frequency of backup and storage (which may be established and connected to the organization's configuration management of information assets) and the retention period for each information asset • the types and forms of information asset retention (paper, CDs, tapes, etc.) • the identification of organization-authorized storage locations and methods, as well as guidelines for appropriate proximity of these storage locations • procedures for accessing stored copies of information assets • standards for the protection and environmental control of information assets in storage (particularly if the assets are stored in locations not owned by the organization) • standards for the testing of the validity of the information assets to be used in restorative activities • periodic revision of the guidelines as operational conditions change The application of these guidelines should be based on the value of the asset and its availability requirements during an emergency, which may be indicated by a service continuity plan. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-9	
Q6	**CERT-RMM Reference** **[KIM:SG4.SP3]** Develop and implement guidelines for the appropriate disposition of information assets. Communicate these guidelines to all staff who are responsible for the resilience of information assets. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations", Page MP-6	
Q7	**CERT-RMM Reference** **[KIM:SG4.SP3]** Communicate these guidelines to all staff who are responsible for theresilience of information assets. 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. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 10-13	
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]	
2	Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	
3	Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[EC:SG1.SP1]** Prioritize facility assets. The prioritization of facility assets is necessary so that the organization can ensure it focuses protection and sustainability activities on facilities that have the most potential for impacting the organization if they are disrupted or destroyed. Unlike other organizational assets, facilities tend to be "hubs" of services; that is, many services tend to be performed in or supported by a single facility. An example of this would be a data center where many application systems (and their associated hardware, software, and network components) support a number of organizational services. Because the loss of a facility can have widespread cascading effects on a number of services, the organization should consider this strongly when prioritizing facility assets. One means for supporting this criterion is to review the mapping between services and facility assets. This information may also be gathered as the result of a business impact analysis activity at the organizational unit level **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems", Page 17	
Q2	**CERT-RMM Reference** **[EC:SG1.SP1]** Periodically validate and update the list of high-value facility assets based on operational and organizational environment changes.	
Q3	**CERT-RMM Reference** **[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. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations", PE-16, PE-17, PE-18	
MIL2-Planned		
1	Is there a documented plan for performing asset management activities?	
2	Is there a documented policy for asset management?	
3	Have stakeholders for asset management activities been identified and made aware of their roles?	
4	Have asset management standards and guidelines been identified and implemented?	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider planning for asset management. This involves developing a plan for performing the process to ensure that an accurate inventory of assets is developed and maintained and can form a foundation for managing operational resilience. Developing and maintaining an asset inventory may be challenging because most organizations have a significant number of assets. Thus, the plan must address how the inventory will be taken and maintained at various levels of the organization. For practicality, most organizations may take inventory at an organizational unit level and have a method or tool to aggregate the inventory at an enterprise level.	
Q2	**CERT-RMM Reference** Consider sponsoring policies and procedures, including the documentation of assets and for establishing asset ownership and custodianship. The asset management policy should address • responsibility, authority, and ownership for performing process activities, including collecting and documenting asset inventory information • the association of assets to core organizational services, and the prioritization of assets in the inventory • methods for measuring adherence to policy, exceptions granted, and policy violations.	
Q3	**CERT-RMM Reference** Consider identifying stakeholders, which are individuals who are involved in various tasks in the asset management process, such as • planning for the process • creating an asset inventory baseline • creating asset profiles • associating assets with services and analyzing asset-service dependencies • reviewing and appraising the effectiveness of process activities • resolving issues in the process	
Q4	**CERT-RMM Reference** Consider sponsoring standards, and guidelines, including procedures, standards, and guidelines for: • documenting asset descriptions and relevant information • describing and identifying asset owners • describing and identifying asset custodians • the development of criteria to provide guidance on asset inventory updating, reconciliation, and change control • the association of assets to core organizational services, and the prioritization of assets in the inventory • methods for measuring adherence to policy, exceptions granted, and policy violations.	

MIL3-Managed		
1	Is there management oversight of the performance of the asset management activities?	
2	Have qualified staff been assigned to perform asset management activities as planned?	
3	Is there adequate funding to perform asset management activities as planned?	
4	Are risks related to the performance of planned asset management activities identified, analyzed, disposed of, monitored, and controlled?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the asset management process as needed to ensure that: • newly acquired assets are included in the inventory • assets that have been modified are reflected accurately in the inventory • assets that have been retired are removed from the inventory • asset-service mapping is accurate and current • ownership and custodianship over assets are established and documented • change control processes are operating appropriately to minimize discrepancies between the organization's asset base and the asset inventory • access to the asset inventory is being limited to only authorized staff • status reports are provided to appropriate stakeholders in a timely manner • asset and service dependency issues are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • administrative, technical, and physical controls are operating as intended • controls are meeting the stated intent of the resilience requirements • actions resulting from internal and external audits are being closed in a timely manner	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in skills required in the asset management process. Examples of these skills include: • knowledge of the tools, techniques, and methods necessary to identify and inventory high-value assets. • knowledge unique to each type of asset that is required to identify and inventory each type • knowledge necessary to work effectively with asset owners and custodians • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective requirements, plans, and programs for the process	

Q3	**CERT-RMM Reference** Consider ensuring that asset management activities are adequately funded. Considerations for funding the asset management process should extend beyond the initial development of the asset inventory to the maintenance of the inventory. Initial costs may be higher if the organization does not have a formal or usable asset baseline to serve as a foundation.	
Q4	**CERT-RMM Reference** Consider managing risk arising from insufficient asset management practices. Discrepancies result when assets are acquired, modified, or retired but not reflected accurately in the asset inventory. Assets form the foundation for operational resilience management, as because they are the target of strategies required to protect and sustain services. To the extent that the asset definition and management process results in inventory discrepancies, the organization's overall ability to manage operational resilience is impeded.	
MIL4-Measured		
1	Are asset management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2	Are asset management activities periodically reviewed to ensure they are adhering to the plan?	
3	Is higher-level management aware of issues related to the performance of asset management?	
Option(s) for Consideration:		
Q1	Consider measuring the asset management process against its process description, standards, and procedures, and address non-compliance.	
Q2	Consider objectively evaluating adherence of the asset management process against its process description, standards, and procedures, and address non-compliance.	
Q3	Consider reviewing the activities, status, and results of the asset management process with higher-level managers and resolve issues.	
MIL5-Defined		
1	Has the organization adopted a standard definition of asset management activities from which operating units can derive practices that fit their unique operating circumstances?	
2	Are improvements to asset management activities documented and shared across the organization?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to asset management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting asset management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Asset Management

2 Controls Management

MIL-1				MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

Goal 1 – Control objectives are established.		
1.	Have control objectives been established for assets (technology, information, facilities, and people) required for delivery of the critical service? [CTRL:SG1.SP1]	
	People	
	Information	
	Technology	
	Facilities	
2.	Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[CTRL:SG1.SP1]** Define and document control objectives that result from management directives and guidelines. Affinity analysis of directives and guidelines may be useful in identifying categories of control objectives. These are examples of control objectives: • prevent unauthorized use of purchase orders • ensure adequate supplies of materials • establish an enterprise architecture for information technology • develop and communicate policies regarding standards of ethical behavior • identify and assess risks that may cause material misstatements of financial records • educate and train staff • manage external entity relationships • establish a compliance program **Additional References** FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems Page 2	

Q2	**CERT-RMM Reference** **[CTRL:SG1.SP1]** The intent of prioritization is to determine the control objectives that most need attention because of their potential to affect operational resilience. 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 (refer to CTRL:SG2, SG3, and SG4). Management directives and guidelines can be used to establish criteria for prioritizing control objectives. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 14-15 Managing for Enterprise Security Page 15	
Goal 2 – Controls are implemented.		
1.	Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[CTRL:SG2.SP1]** Establish enterprise-level controls to satisfy control objectives. These can be a combination of controls that already exist, controls that need to be updated, and new controls that need to be implemented. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 14-15	
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]	
	People	
	Information	
	Technology	
	Facilities	
2.	As a result of the controls analysis, are new controls introduced or existing controls modified to address gaps? [CTRL:SG3.SP1]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[CTRL:SG3.SP1]** Analyze existing controls against control objectives.Identify gaps where enterprise control objectives for the resilience of services and assets and service control objectives are not adequately satisfied by existing controls. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Section 2.4 and Section 3.2	
Q2	**CERT-RMM Reference** **[CTRL:SG3.SP1]** Identify updates to existing controls and proposed new controls to address gaps. This includes identifying gaps where the control objective's priority does not warrant further investment in updated or new controls. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Section 3	
Goal 4 – The internal control system 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]	
	People	
	Information	
	Technology	
	Facilities	
2.	As a result of scheduled assessments, are new controls introduced or existing controls modified to address problem areas? [CTRL:SG4.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[CTRL:SG4.SP1]** Perform control assessments. 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.Various assessment techniques can be used ranging from informal, self-assessments to more structured formal assessments against established standards. Affinity analysis, interviews, and surveys may provide useful insight. In addition, results from business impact analyses, risk assessments, and internal audits and external audits (refer to the Compliance process area) can contribute. **Additional References** Special Publication 800-39 "Managing Information Security RiskOrganization, Mission, and Information System View" Page 46-48	

Q2	**CERT-RMM Reference**	
	[CTRL:SG4.SP1] Identify updates to existing controls and proposed new controls to address problem areas. Organizations can realize efficiencies of scale by requiring specific controls for a given type of asset. For example, standardizing desktop and laptop system configurations or deploying access control systems across a range of technology assets that support multiple high-value services can reduce the cost of controls.	
	Straightforward changes can be addressed by service and asset owners and the line of business and organizational unit managers to whom they report. For more complex changes that require broader organizational planning and coordination, a remediation plan may be required.	
	Remediation plans should address:	
	• the actions the organization must take to ensure that controls satisfy control objectives effectively and efficiently	
	• changes to the internal control system	
	• assignment of responsibility and authority to perform the work	
	• schedule and costs to perform the work	
	• documentation of risk mitigation strategies and residual risks	
	The actions called for in remediation plans must be tracked to closure. Plans are updated as required. Any changes to existing controls and the addition of any new controls may result in the need for a reassessment	
	Additional References	
	Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 48	
MIL2-Planned		
1.	Is there a plan for performing controls management activities?	
2.	Is there a documented policy for controls management?	
3.	Have stakeholders for controls management activities have been identified and made aware of their roles?	
4.	Have controls management standards and guidelines been identified and implemented?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider establishing and maintaining a plan for controls management. The plan for the controls management process should be directly influenced by the management directives and guidelines and resilience requirements that serve as the basis for defining control objectives. The plan for the controls management process should not be confused with remediation plans for changes to the internal control system that require broad organizational planning and coordination. The plan for the controls management process details how the organization will perform controls management, including the development of remediation plans. Subpractice: • Define and document the plan for performing the process. • Define and document the process description. • Review the plan with relevant stakeholders and get their agreement. • Revise the plan as necessary.	

Q2	**CERT-RMM Reference**
	Consider developing a policy for controls management. The controls management policy should address:
	• responsibility, authority, and ownership for performing process activities
	• procedures, standards, and guidelines for
	   - defining and selecting control objectives
	   - prioritizing control objectives
	   - evaluating and acquiring tools for monitoring the performance of controls
	   - analyzing and assessing controls
	   - identifying gaps in controls and approaches for addressing them
	   - identifying redundant and conflicting controls
	   - identifying risks associated with problems in the internal control system
	• periodically assessing the internal control system
	• methods for measuring adherence to policy, exceptions granted, and policy violations	

Q3	**CERT-RMM Reference** Consider identifying and documenting stakeholders of the controls management process. Stakeholders of the controls management process include those that are responsible for control objectives and controls, oversee the controls management process, and are involved in any aspect of ensuring the effectiveness of the internal control system and managing risks resulting from unresolved problems.Stakeholders of the compliance process are also stakeholders of the controls management process for controls that directly support compliance process activities and the fulfillment of compliance obligations.	

Q4	**CERT-RMM Reference**	
	Consider establishing standards and guidelines for controls management.	
	• affinity analysis methods for categorizing control objectives and analyzing controls	
	• methods for prioritizing control objectives	
	• techniques and tools for developing and maintaining traceability between control objectives and controls	
	• methods for conducting surveys and interviews	
	• methods and techniques for identifying and addressing gaps in controls as well as conflicting and	
	redundant controls	
	• methods, techniques, and tools for control analysis and assessment	
	• methods, techniques, and tools for coordinating process activities across organizational units and lines of	
	business	
	• methods, techniques, and tools for collecting, analyzing, validating, and managing information about the	
	internal control system	
	• monitoring, auditing, and other assessment techniques to identify problem areas	
	• methods and tools for managing changes to controls	

MIL3-Managed		
1.	Is there management oversight of the performance of the controls management activities?	
2.	Have qualified staff been assigned to perform controls management activities as planned?	
3.	Is there adequate funding to perform controls management activities as planned?	
4.	Are risks related to the performance of planned controls management activities identified, analyzed, disposed of, monitored, and controlled?	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider conducting oversight of controls management activities. These are examples of controls management work products placed under control: • management directives and guidelines • control objectives and their priorities • enterprise-, service-, and asset-level controls • traceability matrix of control objectives and controls, including responsible staff • analysis and assessment results, including control gaps • updates to existing controls • proposed new controls • redundant and conflicting controls • risks related to unsatisfied control objectives • risks related to redundant and conflicting controls • remediation plans • updates to service continuity plans • process plan • policies and procedures • contracts with external entities	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in the skills necessary to perform controls management. These are examples of skills required in the controls management process: • knowledge of the tools, techniques, and methods necessary to analyze, assess, and manage the internal control system, including those necessary to perform the process using the selected methods, techniques, and tools • knowledge unique to each control objective • knowledge necessary to successfully remediate control gaps, problem areas, redundancies, and conflicts • knowledge necessary to work effectively with asset and service owners and custodians • oral and written communication skills to prepare reports on the effectiveness of the internal control system and defend these reports if required • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective control objectives and controls	
Q3	**CERT-RMM Reference** Consider ensuring that controls management activities are adequately funded. Considerations for funding the process should extend beyond the initial development of controls to the maintenance of the system of internal controls, which includes evaluation of control effectiveness.	
Q4	**CERT-RMM Reference** Consider ensuring that risk arising from the failure of controls management is identified, assessed, and mitigated.	

MIL4-Measured	
1.	Are controls management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are controls management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of controls management?	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider measuring the controls management process. These are examples of metrics for the controls management process: • number of controls and number of controls by category • percentage of control objectives that are fully satisfied by existing controls • percentage of controls that span multiple control objectives • percentage of controls that require updates; percentage of control objectives that are affected by updated controls • percentage of proposed new controls; percentage of control objectives that are affected by proposed new controls • percentage of redundant controls; percentage of control objectives that are affected by redundant controls • percentage of conflicting controls; percentage of control objectives that are affected by conflicting controls • time and resources expended to conduct an analysis of controls (establish the baseline) • time and resources expended to conduct an assessment of controls (periodic) • number of problem areas resulting from the assessment of controls • number of problem areas escalated to higher-level managers for review • percentage of control objectives requiring remediation plans • percentage of controls that have been fully automated • timeliness of resolving control gaps (implementation of control updates and proposed new controls; resolution of redundant and conflicting controls) • reduction in number of controls • number of process risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank) • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	

Q2	**CERT-RMM Reference** Consider reviewing the controls management activities. Periodic reviews of the controls management process are needed to ensure that • control objectives are satisfied and continue to be satisfied across time and in the face of changing business and risk conditions • control problem areas have been identified and remediated • risks related to control problem areas have been identified, properly referred, and addressed • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • actions requiring management involvement are elevated in a timely manner • actions resulting from internal and external audits are being closed in a timely manner	
Q3	**CERT-RMM Reference** Consider reviewing issues with performance of controls management. Reviews of the controls management process may result from periodic assessment or post-event audits that seek to identify problems that must be corrected. Elevating the results of these assessments and audits to managers provides an opportunity to correct controls management process deficiencies and to make managers aware of variations in the process that not only have localized impact but may also affect the organization's resilience as a whole.	
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?	
2.	Are improvements to controls management documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to controls management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	

Q2	**CERT-RMM Reference** Consider collecting controls management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Controls Management

3   Configuration and Change Management

MIL-1			MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

Goal 1 – The life cycle of assets is managed.		
1.	Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]	
	Information	
	Technology	
	Facilities	
2.	Are resilience requirements evaluated as a result of changes to assets? [[RRM:SG1.SP3]	
	Information	
	Technology	
	Facilities	
3.	Is capacity management and planning performed for assets? [TM:SG5.SP3]	
4.	Are change requests tracked to closure? [TM:SG4.SP3]	
5.	Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[ADM:SG3.SP2]** Maintain a requirement change history with rationale for performing the changes. 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. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	

Q2	**CERT-RMM Reference** **[RRM:SG1.SP3]** Evaluate the impact of requirement changes on existing activities and commitments for protecting and sustaining assets and services. 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. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	
Q3	**CERT-RMM Reference** **[TM:SG5.SP3]** Develop a strategy to meet the demand for capacity based on the resilience requirements for the technology asset and the services it supports. In this case, the strategy may need to consider the organization's strategic objectives and how the accomplishment of these objectives affects capacity of current technology assets and future capacity needs. **Additional References** Special Publication 800-128 "Guide for Security Configuration Management of Information Systems" Page 29-30	
Q4	**CERT-RMM Reference** **[TM:SG4.SP3]** Track the status of change requests to closure. Ensure that all change requests have a disposition and that changes that have not been closed are provided an updated status. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	
Q5	**CERT-RMM Reference** **[ADM:SG3.SP2]** Establish communication channels to ensure custodians are aware of changes in assets. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	
Goal 2 – The integrity of technology and information assets is managed.		
1.	Is configuration management performed for technology assets? [TM:SG4.SP2]	
2.	Are techniques in use to detect changes to technology assets? [TM:SG4.SP3]	
3.	Are modifications to technology assets reviewed? [TM:SG4.SP3; TM:SG4.SP.2]	
4.	Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1]	
5.	Is the integrity of information assets monitored? [KIM:SG5SP3]	
6.	Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2; TM:SG4.SP3]	

7.	Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4]	
8.	Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[TM:SG4.SP2]** Create baseline configuration items. 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. **Additional References** Special Publication 800-70 "National Checklist Program for IT Products: Guidelines for Checklist Users and Developers", Entire Document	
Q2	**CERT-RMM Reference** **[TM:SG4.SP3]** Develop and implement change control policies, procedures, and techniques. Change requests address not only new or changed requirements but also maintenance and/or failures in the technology assets. Changes are evaluated to ensure that they are consistent with all technical and resilience requirements. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-2	
Q3	**CERT-RMM Reference** **[TM:SG4.SP2, TM:SG4.SP3]** Review configuration control logs and identify anomalies. Periodically verify (through monitoring and auditing) that changes to configurations are valid and authorized. Analyze the impact of changes proposed in the change requests. Change requests are analyzed to determine the impact that the change will have on the resilience requirements, budget, and schedule. Changes are also evaluated for their impact beyond immediate project or contract requirements. Changes to a technology used in multiple services can resolve an immediate issue while causing a problem in other applications. Obtain agreement and approval for changes to baselines from relevant stakeholders. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	

Q4	**CERT-RMM Reference** **[KIM:SG5.SP1]** Identify and document staff who are authorized to modify information assets, relative to the asset's integrity requirements. This information may be specifically included as part of the information asset's resilience requirements. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" AC-2	
Q5	**CERT-RMM Reference** **[KIM:SG5.SP3]** Establish requirements for the inclusion of data validation controls in services and related systems. The inclusion of data validation controls ensures that information assets retain their integrity when charged into the production cycles of processes and systems. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" PL-1	
Q6	**CERT-RMM Reference** **[TM:SG4.SP2, TM:SG4.SP3]** Perform configuration audits. 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. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3 and CM-9	
Q7	**CERT-RMM Reference** **[TM:SG4.SP4]** Test release builds. 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. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	

Q8	**CERT-RMM Reference** **[TM:SG4.SP1]** Establish access management policies and procedures for requesting and approving access privileges to technology assets.The organization should establish policies and procedures for requesting, approving, and providing access to technology assets to persons, objects, and entities. The access management policy should establish the responsibilities of requestors, asset owners, and asset custodians (who typically are called upon to implement access requests). The policy should address clear guidelines for access requests that originate external to the organization (i.e., from contractors or business partners). The policy should also cover the type and extent of access that will be provided to objects such as systems and processes. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" AC-1	
Goal 3 – Asset configuration baselines are established.		
1.	Do technology assets have configuration baselines? [TM:SG4.SP2]	
2.	Is approval obtained for proposed changes to baselines? [TM:SG4.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[TM:SG4.SP2]** Create baseline configuration items. 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. **Additional References** Special Publication 800-70 "National Checklist Program for IT Products: Guidelines for Checklist Users and Developers" Page Entire Document	
Q2	**CERT-RMM Reference** **[TM:SG4.SP3]** Obtain agreement and approval for changes to baselines from relevant stakeholders. **Additional Reference** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CM-3	
MIL2-Planned		
1.	Is there a documented plan for performing change management activities?	
2.	Is there a documented policy for change management?	

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

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider planning for configuration and change management. The plan for configuration and change management should maintain a focus of ensuring adequate protection and sustainment strategies as assets are deployed and are modified.	
Q2	**CERT-RMM Reference** Consider sponsoring policies and procedures, including the documentation of configuration and changes. The configuration and change policy should address • configuration baselines, baseline review and change criteria, change request management, change testing, change risk assessment, and change deployment. • methods for measuring adherence to policy, exceptions granted, and policy violations.	
Q3	**CERT-RMM Reference** Consider identifying stakeholders, which are individuals who are involved in various tasks in the configuration and change management process, such as • planning for the process • creating baseline configurations • evaluating an updating changes • managing changes to assets and to the asset inventory • reviewing and appraising the effectiveness of process activities • resolving issues in the process	
Q4	**CERT-RMM Reference** Consider sponsoring standards, and guidelines, including procedures, standards, and guidelines for • establishing and managing baseline configurations • change control • methods for measuring adherence to policy, exceptions granted, and policy violations.	
MIL3-Managed		
1.	Is there management oversight of the performance of the change management activities?	
2.	Have qualified staff been assigned to perform change management activities as planned?	
3.	Is there adequate funding to perform change management activities as planned?	
4.	Are risks related to the performance of planned change management activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the configuration and change management process are needed to ensure that • assets are placed under configuration management • baseline configurations meet the organization's needs • baseline configurations are updated as needed • changes to assets do not introduce unacceptable risk • changes to assets are effectively communicated to all who need to know	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in skills required in the configuration and change management process. Examples of these skills include: • knowledge of the tools, techniques, and methods necessary to manage baseline configurations. • knowledge necessary to work effectively with asset owners and custodians • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective requirements, plans, and programs for the process	
Q3	**CERT-RMM Reference** Consider ensuring that configuration and change management activities are adequately funded. Funding the configuration and change management process should include ensuring that baseline configurations are available to all stakeholders who require access, that baseline configurations are appropriately managed under the change control process. The change control process should be funded to ensure that all stakeholders are aware of changes, that changes are sufficiently tested, and that unacceptable risk is not introduces to the operating environment as a result of changes.	
Q4	**CERT-RMM Reference** Consider managing risk arising from insufficient configuration and change management practices. Discrepancies result when assets are acquired, modified, or retired but not reflected accurately in the change management repository, or when assets are deployed without being placed under configuration management. Assets form the foundation for operational resilience management, as because they are the target of strategies required to protect and sustain services. To the extent that the asset's configuration is not under configuration management, the organization's overall ability to manage operational resilience is impeded.	
MIL4-Measured		
1.	Are change management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are change management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of change management?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider Objectively evaluating adherence of the configuration and change management process against its process description, standards, and procedures, and address non-compliance.	
Q2	**CERT-RMM Reference** Consider reviewing activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues. Reviews of the configuration and change management process may result from periodic examination or post-event audits that seek to identify problems that must be corrected. Elevating the results of these examinations to managers provides an opportunity to correct process deficiencies and to make managers aware of variations in the risk management process that not only have localized impact but may also affect the organization's resilience as a whole.	
Q3	**CERT-RMM Reference** Consider objectively evaluating adherence of the configuration and change management process against its process description, standards, and procedures, and address non-compliance.	
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?	
2.	Are improvements to change management documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to configuration and change management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	

| Q2 | **CERT-RMM Reference**
Collect configuration and change management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets. These are examples of improvement work products and information:
• metrics and measurements of the viability of the process
• changes and trends in operating conditions that affect risk sources and categories
• changes in risk conditions and the risk environment that affect risk parameters, measurement criteria, or risk dispositions
• lessons learned in post-event review of continuity exercises, incidents, and disruptions in continuity,   particularly those that result in losses or compromises that exceed risk parameters and measurement criteria
• process lessons learned that can be applied to improve operational resilience management performance   and internal controls
• issues with the risk identification, analysis, prioritization, overall assessment, mitigation, and monitoring   processes
• lessons learned from both successfully and unsuccessfully mitigating identified risks
• risk mitigation plan costs and benefits for future return on investment analysis
• resilience requirements that are not being satisfied or are being exceeded | |

Other Observations – Configuration and Change Management

4 Vulnerability Management

MIL-1				MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

Goal 1 – Preparation for vulnerability analysis and resolution activities is conducted.	
1. Has a vulnerability analysis and resolution strategy been developed? [VAR: SG1.SP2]	
People	
Information	
Technology	
Facilities	
2. Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR: SG1.SP2]	
People	
Information	
Technology	
Facilities	
Option(s) for Consideration:	
Q1 **CERT-RMM Reference** **[VAR: SG1.SP2]** Develop and document an operational vulnerability analysis and resolution strategy. 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 **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 6-9	

Q2	**CERT-RMM Reference** **[VAR: SG1.SP2]** Identify the tools, techniques, and methods that the organization will use to identify vulnerabilities to assets. 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 **Additional References** Special Publication 800-40 Version 3 "Creating a Patch Management and Vulnerability Management Program" Section 4	
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	
	Technology	
	Facilities	
2.	Is the information from these sources kept current? [VAR: SG2.SP1]	
	Information	
	Technology	
	Facilities	
3.	Are vulnerabilities being actively discovered? [VAR: SG2.SP2]	
	Information	
	Technology	
	Facilities	
4.	Are vulnerabilities categorized and prioritized? [VAR: SG2.SP3]	
	Information	
	Technology	
	Facilities	
5.	Are vulnerabilities analyzed to determine relevance to the organization? [VAR: SG2.SP3]	
	Information	
	Technology	
	Facilities	
6.	Is a repository used for recording information about vulnerabilities and their resolution? [VAR: SG2.SP2]	
	Information	
	Technology	
	Facilities	

	Option(s) for Consideration:	
Q1	CERT-RMM Reference **[VAR: SG2.SP1]** Identify sources of relevant vulnerability information. The sources of vulnerability information should fit the organization's vulnerability identification and analysis needs. The internal sources of vulnerability information supplied by other operational resilience management processes should be included in the list. **Additional References** Special Publication 800-40 Version 3"Creating a Patch Management and Vulnerability Management Program" Section 3	
Q2	**CERT-RMM Reference** **[VAR: SG2.SP1**] Review sources on a regular basis and update as necessary. 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. **Additional References** Special Publication 800-40 Version 3 "Creating a Patch Management and Vulnerability Management Program" Section 3	
Q3	**CERT-RMM Reference** **[VAR: SG2.SP2]** Discover vulnerabilities.Data collection should be coordinated to discover vulnerabilities and populate the vulnerability repository as efficiently as possible. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 33	
Q4	**CERT-RMM Reference** **[VAR: SG2.SP3]** Prioritize and categorize vulnerabilities for disposition. Based on the organization's prioritization guidelines and the results of vulnerability analysis, vulnerabilities must be categorized by disposition. **Additional References** Special Publication 800-40 Version 3 "Creating a Patch Management and Vulnerability Management Program" Section 3	
Q5	**CERT-RMM Reference** **[VAR: SG2.SP3]** Analyze the structure and action of the vulnerability. This may require the vulnerability to be decomposed into other artifacts such as threat, threat actor, motive, and potential outcome. In addition, relationships between vulnerabilities may be identified that could indicate similar root causes or origins that must be considered in resolution actions.	

Q6	**CERT-RMM Reference** **[VAR: SG2.SP2]** Establishes a vulnerability repository as the central source of vulnerability life-cycle information and populate the vulnerability repository. 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 **Additional References** Special Publication 800-40 Version 3 "Creating a Patch Management and Vulnerability Management Program" Section 4	
Goal 3 – Exposure to identified vulnerabilities is managed.		
1.	Are actions taken to manage exposure to identified vulnerabilities? [VAR: SG3.SP1]	
2.	Is the effectiveness of vulnerability mitigation reviewed? [VAR: SG3.SP1]	
3.	Is the status of unresolved vulnerabilities monitored? [VAR: SG3.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[VAR: SG3.SP1]** Develop a vulnerability management strategy for all vulnerabilities that require resolution. The strategy should address the actions that the organization will take to reduce or eliminate exposure or to provide an operational workaround if preferable. **Additional References** Special Publication 800-40 Version 2.0 "Creating a Patch Management and Vulnerability Management Program"	
Q2	**CERT-RMM Reference** **[VAR: SG3.SP1]** Analyze the effectiveness of vulnerability management strategies to ensure that objectives are achieved. **Additional References** Special Publication 800-40 Version 3 "Creating a Patch Management and Vulnerability Management Program" Section 5	

Q3	**CERT-RMM Reference** **[VAR: SG3.SP1]** Monitor the status of open vulnerabilities. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 33	
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]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[VAR: SG4.SP1]** Identify and analyze the root causes of vulnerabilities. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 39	
MIL2-Planned		
1.	Is there a documented plan for performing vulnerability management activities?	
2.	Is there a documented policy for vulnerability management?	
3.	Have stakeholders for vulnerability management activities been identified and made aware of their roles?	
4.	Have vulnerability management standards and guidelines been identified and implemented?	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference**Consider establishing and managing a plan for vulnerability management. The plan for the vulnerability management process should not be confused with the organizational vulnerability management strategy and plan for identifying and analyzing vulnerabilities. The plan for the vulnerability management process details how the organization will perform vulnerability analysis and resolution, including the development of strategies and plans for vulnerability analysis and resolution.	

Q2	**CERT-RMM Reference**
	Consider developing a policy for vulnerability management. The vulnerability management policy should address
	• responsibility, authority, and ownership for performing process activities
	• information categorization, labeling, and handling
	• protection against tampering or unauthorized access
	• encryption, secure storage, and secure transport and distribution of information
	• procedures, standards, and guidelines for
	  - identifying the assets that are the focus of vulnerability management activities
	  - storage capacity of collection mechanisms and actions to take if capacity is exceeded by type of media
	  - collection of vulnerability data
	  - recording and storage of vulnerability data, including collection media (electronic logs, data files,
	    databases, and information repositories)
	  - distribution of vulnerability data, including media, methods, and channels
	  - service level agreement terms and conditions for external entities involved in process activities
	• methods for measuring adherence to policy, exceptions granted, and policy violations	

| Q3 | **CERT-RMM Reference**Consider identifying stakeholders of the vulnerability management process. These are examples of stakeholders of the vulnerability analysis and resolution process:
• higher-level managers responsible for establishing organizational risk criteria and tolerances
• staff responsible for the organization's risk management plan• asset owners, custodians, and users
• staff responsible for managing operational risks to assets
• staff responsible for establishing, implementing, and maintaining an internal control system for assets
• staff responsible for developing, testing, implementing, and executing service continuity plans
• external entities responsible for managing high-value assets and providing essential services
• internet service providers
• human resources (for people assets)
• legal counsel
• information technology staff, such as system administrators and CSIRTs
• staff responsible for physical security (for facility assets)
• internal and external auditors
• owners of operational resilience management processes, including risk management, incident management and control, and service continuity | |
| Q4 | **CERT-RMM Reference**

Consider developing standards and guidelines for vulnerability management. Such standards and guidelines should address:
• vulnerability data
• process strategy and plans, including the scope of the plans and commitments to the plans
• list of sources of vulnerability information
• list of internal and external stakeholders and a plan for their involvement
• vulnerability prioritization guidelines
• prioritized process requirements, accepted requirements, and risks resulting from unsatisfied requirements
• infrastructure requirements
• vulnerability data collection and storage standards and parameters
• vulnerability data identification, monitoring, collection, analysis, remediation, handling, and storage   methods, procedures, techniques, and tools
• vulnerability data distribution plans, procedures, processes, media, methods, and tools
• collection media, including electronic logs, data files, databases, and repositories
• vulnerability status reports, including resolution strategies
• policies and procedures
• contracts with external entities | |

MIL3-Managed	
1.	Is there management oversight of the performance of the vulnerability management activities?	
2.	Have qualified staff been assigned to perform vulnerability management activities as planned?	
3.	Is there adequate funding to perform vulnerability management activities as planned?	
4.	Are risks related to the performance of planned vulnerability management activities identified, analyzed, disposed of, monitored, and controlled?	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider conducting reviews of the vulnerability management process, including: • current sources of vulnerability data are in use • assets subject to the process are identified, documented, and included in the scope of process activities • assets that have been retired are removed from the scope of the process • vulnerability data is identified, collected, and stored in a timely manner • the vulnerability repository is established and maintained • access to the vulnerability repository is limited to authorized staff • vulnerability management status reports are provided to appropriate stakeholders in a timely manner • vulnerabilities are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • administrative, technical, and physical controls are operating as intended • controls are meeting the stated intent of the resilience requirements • actions resulting from internal and external audits are being closed in a timely manner	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff possess adequate skills to perform vulnerability management activities. These are examples of skills required in the vulnerability management process: • knowledge of tools, techniques, and methods used to identify, analyze, remediate, monitor, and communicate vulnerabilities for all asset types, including those necessary to perform the process using the selected methods, techniques, and tools • knowledge of tools, techniques, and methods necessary to ensure the confidentiality, integrity, and availability of vulnerability data • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements, plans, and programs • knowledge necessary to analyze and prioritize process requirements • knowledge necessary to interpret vulnerability data and represent it in ways that are meaningful and appropriate for managers and stakeholders	

Q3	**CERT-RMM Reference** Consider ensuring that vulnerability management activities are adequately funded. Funding the process should extend beyond the initial development of vulnerability management activities, tools, and processes to ensure that the operating environment is continuously monitored for vulnerabilities.	
Q4	**CERT-RMM Reference** Consider managing risk from the failure of vulnerability management processes. Monitor key components of vulnerability management, including: • current sources of vulnerability data are in use • assets subject to the process are identified, documented, and included in the scope of process activities • assets that have been retired are removed from the scope of the process • vulnerability data is identified, collected, and stored in a timely manner • the vulnerability repository is established and maintained • access to the vulnerability repository is limited to authorized staff • vulnerability management status reports are provided to appropriate stakeholders in a timely manner • vulnerabilities are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • administrative, technical, and physical controls are operating as intended • controls are meeting the stated intent of the resilience requirements • actions resulting from internal and external audits are being closed in a timely manner	

MIL4-Measured		
1.	Are vulnerability management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are vulnerability management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of vulnerability management?	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider measuring the vulnerability management process. These are examples of metrics for the vulnerability management process: • for high-value information, technology, and facilities assets (including assets owned and managed by external entities as well as internally): • number of high-value assets (by type) subject to process activities (This is determined by the resilience requirements associated with identified assets and assumes an up-to-date asset inventory. • percentage of high-value assets that have been monitored for vulnerabilities within an agreed-upon time interval • percentage of high-value assets that have been audited or assessed for vulnerabilities within an agreed upon time interval • number of reported vulnerabilities by asset type or category for which some form of resolution or remediation is called for (course of action, reduction, elimination) • percentage of vulnerabilities that have been satisfactorily remediated (or conversely, percentage of open vulnerabilities) by time interval (days, weeks, months) • number of reported vulnerabilities for which a vulnerability management strategy exists • percentage of vulnerabilities with a vulnerability management strategy that is on track per plan • number and percentage of vulnerabilities requiring a root-cause analysis • number of vulnerabilities referred to the risk management process; number of vulnerabilities where corrective action is still pending (by risk rank) • number of vulnerabilities referred to the incident management and control process by time interval • number of vulnerabilities referred to the service continuity process by time interval • schedule for collecting, recording, and distributing vulnerability data, including elapsed time from high-value data collection to data distribution to key stakeholders • percentage of organizational units, lines of business, projects, and activities using vulnerability data to assess the performance of operational resilience management processes • number of risks resulting from unsatisfied process requirements, designated as high, medium, or low or some other organizational risk ranking method • number of scope changes to process activities by time interval • number of process risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank) • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	

Q2	**CERT-RMM Reference** Consider objectively evaluating adherence of the vulnerability management process against its process description, standards, and procedures, and address non-compliance. These are examples of activities to be reviewed: • the alignment of stakeholder requirements and needs with the process scope, strategy, plans, and management strategies for specific vulnerabilities • assignment of responsibility, accountability, and authority for process activities • determining the adequacy of process reports and reviews in informing decision makers regarding the performance of operational resilience management activities and the need to take corrective action, if any • verification of data confidentiality, integrity, and availability controls • use of process data for improving strategies for protecting and sustaining assets and services	
Q3	**CERT-RMM Reference** Consider ensuring that the organization Reviews the activities, status, and results of the vulnerability management process with higher-level managers and resolves issues.	
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?	
2.	Are improvements to vulnerability management activities documented and shared across the organization?	
Option(s) for Consideration:		

Q1	**CERT-RMM Reference**
	Consider establishing an organization-wide approach to vulnerability management, that includes:
	• Selecting from the organization's set of standard processes those processes that cover the asset definition
	   and management process and best meet the needs of the organizational unit or line of business.
	• Establishing the defined process by tailoring the selected processes according to the organization's
	   tailoring guidelines.
	• Ensuring that the organization's process objectives are appropriately addressed in the defined process,
	   and ensure that process governance extends to the tailored processes.
	• Documenting the defined process and the records of the tailoring.
	• Revising the description of the defined process as necessary.	

Q2	**CERT-RMM Reference** Consider Collecting vulnerability management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Vulnerability Management

5 Incident Management

MIL-1					MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

	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]	
2.	Is the incident management plan reviewed and updated? [IMC:SG1.SP1]	
3.	Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	
4.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[IMC:SG1.SP1]** Establish the incident management plan. 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 **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Handbook for Computer Security Incident Response Teams (CSIRTs)	
Q2	**CERT-RMM Reference** **[IMC:SG1.SP1]** Revise the plan and commitments as necessary **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" IR-8	
Q3	**CERT-RMM Reference** **[IMC:SG1.SP2]** Develop detailed job descriptions for each role and responsibility detailed in the incident management plan. **Additional References**	

	Special Publication 800-61 "Computer Security Incident Handling guide" Section 2.4 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 41	
Q4	**CERT-RMM Reference** **[IMC:SG1.SP2]** Assign staff to incident management roles and responsibilities. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 2.4 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 41	
Goal 2 – A process for detecting, reporting, triaging, and analyzing events established.		
1.	Are events detected and reported? [IMC:SG2.SP1]	
2.	Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]	
3.	Are events categorized? [IMC:SG2.SP4]	
4.	Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4]	
5.	Are events prioritized? [IMC:SG2.SP4]	
6.	Is the status of events tracked? [IMC:SG2.SP4]	
7.	Are events tracked to resolution? [IMC:SG2.SP4]	
8.	Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3]	
9.	Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[IMC:SG2.SP1]** Define the methods of event detection and reporting. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 2.3 Handbook for Computer Security Incident Response Teams (CSIRTs)	
Q2	**CERT-RMM Reference** **[IMC:SG2.SP2]** Develop and implement an incident management knowledgebase that allows for the entry of event reports (and the tracking of declared incidents) through all phases of their life cycle.Guidelines and standards for the consistent documentation of events should be developed and communicated to all who are involved in the reporting and logging processes. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 2 Handbook for Computer Security Incident Response Teams (CSIRTs)	

Q3	**CERT-RMM Reference** **[IMC:SG2.SP4]** Assign a category to events from the organization's standard category definitions. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 66	
Q4	**CERT-RMM Reference** **[IMC:SG2.SP4]** Perform correlation analysis on event reports to determine if there is affinity between two or more events. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.4 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 69-70	
Q5	**CERT-RMM Reference** **[IMC:SG2.SP4]** Prioritize events. Events may be prioritized based on event knowledge, the results of categorization and correlation analysis, incident declaration criteria and experience with past-declared incidents. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.2 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 124-128	
Q6	**CERT-RMM Reference** **[IMC:SG2.SP4]** Assign events that have not been assigned a "closed" status for furtheranalysis and resolution. Possible dispositions 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 **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3Handbook for Computer Security Incident Response Teams (CSIRTs) Page 153	
Q7	**CERT-RMM Reference** **[IMC:SG2.SP4]** Periodically review the incident knowledgebase for events that have not been closed or for which there is no disposition. Events that have not been closed or that do not have a disposition should be reprioritized and analyzed for resolution. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.4 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 155-156	

Q8	**CERT-RMM Reference** **[IMC:SG2.SP3]** Identify relevant rules, laws, regulations, and policies for which incident evidence may be required. Because there may be compliance issues related to the collection and preservation of incident data, this practice must be considered in the context of the organization's compliance program. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 2.4.4 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 26	
Q9	**CERT-RMM Reference** **[IMC:SG2.SP3]** Document events and related evidence information in the incident management knowledgebase where practical. Rules, laws, regulations, and policies may require specific documentation for forensic purposes. These specific requirements must be included in the organization's logging and tracking process. Some information about events may be confidential or sensitive, so the organization must be careful to appropriately limit access to event information to only those who need to know about it **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 26	
Goal 3 – Incidents are declared and analyzed.		
1.	Are incidents declared? [IMC:SG3.SP1]	
2.	Have criteria for the declaration of an incident been established? [IMC.SG3.SP1]	
3.	Are incidents analyzed to determine a response? [IMC:SG3.SP2]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[IMC:SG3.SP1]** Establish a process to declare incidents. 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. The time from event detection to incident declaration may be immediate, requiring little additional review and analysis. In other cases, incident declaration requires more thoughtful analysis **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.2 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 77-79	
Q2	**CERT-RMM Reference** **[IMC.SG3.SP1]** Establish incident declaration criteria for use in guiding when to declare an incident. 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. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.2.6 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 77-79	
Q3	**CERT-RMM Reference** **[IMC:SG3.SP2]** Identify relevant analysis tools, techniques, and activities that the organization will use to analyze incidents and develop appropriate responses. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.1.1 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 79-91	
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]	
2.	Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]	
3.	Are incident status and response communicated to affected parties? [IMC:SG4.SP3]	
4.	Are incidents tracked to resolution? [IMC:SG4.SP4]	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[IMC:SG4.SP1]** Develop incident escalation procedures.Incident escalation procedures should consider the type and extent of incident and the appropriate stakeholders 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. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.2.6 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 128-132

Q2	**CERT-RMM Reference**
	[IMC:SG4.SP2] Develop an incident response strategy and plan to limit incident effect and to repair incident damage. The incident response strategy and plan should address at a minimum
	• the essential activities (administrative, technical, and physical) that are required to contain or limit
	  damage and provide service continuity
	• existing continuity of operations and restoration plans in the organization's plan inventory
	• the resources and skills required to perform the incident response strategy and plan
	• coordination activities with other internal staff and external agencies that must be performed to
	  implement the strategy
	• the levels of authority and access needed by responders to carry out the strategy and plan
	• objectives for measuring when the strategy and plan are successful
	• the estimated cost of implementing the strategy and plan
	• the essential activities necessary to restore services to normal operation (recovery), the resources
	  involved in these activities, and their estimated cost
	• legal and regulatory obligations that must be met by the strategy
	• standardized responses for certain types of incidents
	
	Additional References
	Special Publication 800-61 "Computer Security Incident Handling guide" Section 3.1

Q3	**CERT-RMM Reference** **[IMC:SG4.SP3]** Develop and implement an organizational incident management communications plan. The incident communications plan should address the stakeholders with whom communications about incidents are required. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Section 2.3.1 Handbook for Computer Security Incident Response Teams (CSIRTs) Page 92-99

Q4	**CERT-RMM Reference** **[IMC:SG4.SP4]** Track incidents that have been open for an extended period of time without closure and resolve. 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. **Additional References** Special Publication 800-61 "Computer Security Incident Handling guide" Handbook for Computer Security Incident Response Teams (CSIRTs)	
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]	
2.	Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	
3.	Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[IMC:SG5.SP1]** Identify root-cause analysis tools and techniques and ensure all staff who participate in analysis are trained in their use. These tools and techniques may include cause-and-effect diagrams, interrelationship diagrams, causal factor tree analysis, etc. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" IR-8	
Q2	**CERT-RMM Reference** **[IMC:SG5.SP2]** Establish a problem management system to ensure that all operational events that are not part of standard operation (incidents, problems, and errors) are recorded, analyzed, and resolved in a timely manner. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" IR-1	

Q3	**CERT-RMM Reference** **[IMC:SG5.SP3]** Review incident knowledgebase information and update the following areas accordingly: • protection strategies and controls for assets involved in the incident • continuity plans and strategies for sustaining assets involved in the incident • information security and other organizational policies that need to reflect new standards, procedures, and guidelines based on what is learned in the incident handling • training for staff on information security, business continuity, and IT operations **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" IR-4	
MIL2-Planned		
1.	Is there a documented plan for performing incident management activities?	
2.	Is there a documented policy for incident management?	
3.	Have stakeholders for incident management activities been identified and made aware of their roles?	
4.	Have incident management standards and guidelines been identified and implemented?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing a plan for incident management. The plan for the incident management and control process should reflect the organization's stated philosophy of incident management and the preferred means for handling incidents (i.e., through a dedicated or permanent team, a virtual team, etc.). Subpractice: • Define and document the plan for performing the process. • Define and document the process description. • Review the plan with relevant stakeholders and get their commitment. • Revise the plan as necessary.	
Q2	**CERT-RMM Reference** These are examples of tools, techniques, and methods to support the incident management process: • methods, techniques, and tools for - event identification, detection, and reporting - analyzing events and incidents, including determining when one or more events should be declared an incident - collecting, documenting, and preserving evidence for events and incidents - recovering from events • methods and tools for event and incident logging and tracking • methods for triaging events • root-cause analysis techniques and tools, such as cause-and-effect diagrams, interrelationship diagrams, and causal factor tree analysis	

	• incident databases and knowledge bases, including predetermined response and recovery actions for specific types of incidents • methods and techniques for responding to events • communications methods for reporting and escalating incidents • methods for conducting post-incident reviews and ensuring lessons learned are reflected in process activities
Q3	**CERT-RMM Reference** Consider identifying stakeholders of the incident management process. Examples include: • incident owners • asset owners and custodians • service owners • organizational unit and line of business managers responsible for high-value assets and the services they support • staff who serve key roles in incident communications activities, such as public relations • staff who provide input to and resolution of incidents as they are escalated • staff responsible for developing, implementing, and managing an internal control system for assets • external entities involved in process activities and responsible for managing high-value assets • human resources • information technology staff • service desk staff • staff responsible for physical security • legal and law enforcement staff, including federal agencies • internal and external auditors • regulatory and governing agencies

Q4	**CERT-RMM Reference**	
	Consider developing standards and guidelines for incident management activities. Such standards and guidelines should include information on: • event reports, including sources of event detection and reporting • incident management plans and the process plan • incident response strategy and plan • event and incident status reports • incident communications plan • list of incident stakeholders • incident management policies, procedures, standards, and guidelines • incident knowledgebase • event and incident evidence • incident declaration criteria • incident escalation procedures and criteria • post-incident analysis reports • list of incident management process improvements • contracts with external entities	
MIL3-Managed		
1.	Is there management oversight of the performance of the incident management activities?	
2.	Have qualified staff been assigned to perform incident management activities as planned?	
3.	Is there adequate funding to perform incident management activities as planned?	
4.	Are risks related to the performance of planned incident management activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the incident management process. Periodic reviews are needed to ensure that • the process is known and accessible • events and incidents are identified, reported, and addressed on a timely basis • events and incidents are logged and closed • proper forensic procedures are used to collect and preserve evidence • events are properly triaged and analyzed for root causes • incidents are properly declared • incidents are properly escalated to designated stakeholders • incident response capabilities are commensurate with the priority of an incident • incidents are communicated appropriately to stakeholders at a level commensurate with their involvement • event and incident status reports are provided to appropriate stakeholders in a timely manner • post-incident reviews are performed to improve the process • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • administrative, technical, and physical controls are operating as intended • controls are meeting the stated intent of the resilience requirements • actions resulting from internal and external audits are being closed in a timely manner	

Q2	**CERT-RMM Reference**	
	Consider ensuring that responsible staff are trained in skills required in the incident management process. Examples of these skills include: • event detection, reporting, and tracking, including service desk activities • documenting and logging event reports • collecting and preserving evidence • technical analysis of events and incidents, including triage • declaring incidents • escalating and communicating incidents • understanding and applying laws, rules, and regulations • performing incident response, including damage containment • creating, managing, and deploying incident response teams • developing and implementing administrative, technical, and physical controls • performing root-cause analysis and post-incident review • using tools, techniques, and methods necessary to handle incidents throughout their life cycle, including those necessary to perform the process using the selected methods, techniques, and tools • knowledge unique to each type of asset or service that may be the target of an incident • working effectively and collaborating with asset owners and custodians • eliciting and prioritizing stakeholder requirements and needs and interpreting them to develop effective incident management plans and plans for handling specific types of incidents	
Q3	**CERT-RMM Reference**	
	Consider ensuring that incident management activities are adequately funded. Considerations for funding the process should extend beyond the initial development of incident management activities, tools, and processes to ensure that the organization maintains a capability to manage incidents.	
Q4	**CERT-RMM Reference**	
	Consider managing risk from the failure of the incident management process. Failures can occur in: • detecting events and incidents • planning for incident handling, management, and response • making commitments to process plans and activities • collecting, documenting, and preserving event and incident evidence • analyzing events and incidents • declaring incidents • responding to incidents, including participating on incident response teams • communicating events and incidents and the status of incidents as they move through the incident lifecycle • escalating incidents • coordinating process activities • reviewing and appraising the effectiveness of process activities • performing post-incident review and improvement processes	

MIL4-Measured		
1.	Are incident management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are incident management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of incident management?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider measuring the performance of incident management activities. Include • percentage of operational time that high-value services and assets were unavailable (as seen by users and customers) due to incidents • percentage of incidents that exploited existing vulnerabilities with known solutions, patches, or workarounds • number and percentage of events or incidents handled in a specific period • number and percentage of events or incidents that are contained in a specific period • percentage of incidents that require escalation • percentage of incidents that require involvement of law enforcement • number of events or incidents that have been logged but not closed • average time between event detection and related incident declaration, response, or closure • percentage increase in the volume of events and incidents in a specific period • extent of consequences to the organization due to incidents by incident type (also referred to as "magnitude") • percentage increase in the elapsed time of the incident life cycle by incident type • number and percentage of recurrence of specified events or incidents • percentage increase in resource needs (training, skill building, additional human resources) to support incident management • number of post-incident review activities that result in control changes or improvements to the process • number of incidents referred to the risk management process; number of risks where corrective action is still pending (by risk rank) • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	
Q2	**CERT-RMM Reference** Consider objectively evaluating adherence of the incident management and control process against its process description, standards, and procedures, and address non-compliance.	

Q3	**CERT-RMM Reference** Consider ensuring that the organization Reviews the activities, status, and results of the incident management process with higher-level managers and resolves issues.	
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?	
2.	Are improvements to incident management activities documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to incident management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting incident management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Incident Management

6 Service Continuity Management

MIL-1				MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

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]	
People	
Information	
Technology	
Facilities	
2. Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2]	
3. Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	
4. Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	
5. Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	
6. Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1]	
Option(s) for Consideration:	
Q1 **CERT-RMM Reference** **[SC:SG3.SP2]** Document the service continuity plans using available templates as appropriate. A service continuity plan typically includes the following information: • identification of authority for initiating and executing the plan (plan ownership) • identification of the communication mechanism to initiate execution of the plan **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page A.3-1 - A.3-10	

Q2	**CERT-RMM Reference** **[SC:SG3.SP2]** Document the key elements of the specific plan. Documentation of the plan must be consistent with the standards and guidelines established by the organization to ensure plan consistency, accuracy, and ability to implement. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page A.3-1 - A.3- 10	
Q3	**CERT-RMM Reference** **[SC:SG3.SP3]** Assign staff to the service continuity plans. Ensure that those who are assigned tasks in the plans are aware of their assignments, have the authority to act as prescribed in the plans, and are held accountable for their activities. Ensure that these staff members commit to performing their roles as described in the plans **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-2	
Q4	**CERT-RMM Reference** **[SC:SG2.SP2]** Develop a key contact list for organizational services that can be included as part of the service continuity plans. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page 31-33	
Q5	**CERT-RMM Reference** **[SC:SG3.SP4]** Store and protect the service continuity plans in the plan inventory or database. Ensure that the service continuity plans are properly protected but accessible on demand to those who have proper authorization.	

Q6	**CERT-RMM Reference** Establish availability metrics for high-value technology assets. Availability metrics establish the planned and required "uptime" for a technology asset. They are typically established as part of the asset's resilience requirement for availability and may be developed with consideration of the services that the asset supports. While availability metrics are most useful for managing technology assets in operation, they also play a significant part in the development plans to sustain technology assets in that they establish a parameter or target that must be attained by technology assets under disruptive conditions. In other words, the availability metric must be met by an asset not only in day-to-day operations but sometimes also under diminished conditions brought on by a disruption or event. These metrics must be considered in planning to determine whether they can be met under diminished conditions and, if not, what additional steps the organization may need to take (i.e., implement manual procedures) to ensure that associated services are not affected. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page 16-18	
Goal 2 – Service continuity plans are reviewed to resolve conflicts between plans.		
1.	Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** [SC:SG4.SP2] Review plans to determine plan conflicts. Determine the severity of plan conflicts and develop appropriate mitigation actions to reduce or eliminate the conflicts. Conflicts that would impede successful plan execution pose operational risks that must be mitigated by the organization. Remember that the conflict may affect more than one plan, and therefore mitigation actions may have to be performed on more than one plan.	
Goal 3 - Service continuity plans tested to ensure they meet their stated objectives.		
1.	Have standards for testing service continuity plans been implemented? [SC:SG5.SP1]	
2.	Has a schedule for testing service continuity plans been established? [SC:SG5.SP1]	
3.	Are service continuity plans tested? [SC:SG5.SP3]	
4.	Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1]	
5.	Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[SC:SG5.SP1]** Develop a testing program and test standards to apply universally across all testing of service continuity plans. **Additional References** Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" Page 2-1 - 2-5	
Q2	**CERT-RMM Reference** **[SC:SG5.SP1]** Establish schedules for ongoing testing and review of plans. **Additional References** Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" Page 6-1	
Q3	**CERT-RMM Reference** **[SC:SG5.SP3]** Execute the service continuity plan test. 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. **Additional References** Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" Page 6-1 - 6-6	
Q4	**CERT-RMM Reference** **[KIM:SG6.SP1]** Periodically test the organization's backup and storage procedures and guidelines to ensure continued validity as operational conditions change. Stored information assets should be periodically tested to ensure that they are complete, accurate, and current and can be used for restorative purposes when necessary. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-9 and CP-10	
Q5	**CERT-RMM Reference** **[SC:SG5.SP4]** Compare actual test results with expected test results and 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. **Additional References** Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities" Page 6-6	

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]	
2.	Is the execution of service continuity plans reviewed? [SC:SG6.SP2]	
3.	Are improvements identified as a result of executing service continuity plans? (SC:SG7.SP2)	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[SC:SG6.SP1]** Determine the conditions under which a service continuity plan must be executed. Ensure that the owners of service continuity plans understand these conditions and have the authority and responsibility to execute the plans if necessary. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page 36	
Q2	**CERT-RMM Reference** **[SC:SG6.SP2]** Compare documented service continuity plan results with plan objectives and expectations. 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.	
Q3	**CERT-RMM Reference** **[SC:SG7.SP2]** Identify and document changes to service continuity plans based ondefined criteria and conditions such as the results of service continuity plan execution or testing **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems"	

MIL2-Planned		
1.	Is there a documented plan for performing service continuity activities?	
2.	Is there a documented policy for service continuity?	
3.	Have stakeholders for service continuity activities been identified and made aware of their roles?	
4.	Have service continuity standards and guidelines been identified and implemented?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing a plan for Service Continuity management. Such a plan includes information on how the organization will carry out service continuity planning and execution. A plan for service continuity is an organizational construct from which a service continuity program is developed and implemented. The plan for the service continuity process should be directly influenced by the strategic planning process of the organization and reflect strategic initiatives where appropriate. The plan for the service continuity process should not be confused with a plan (and program) for service continuity or service-specific continuity plans. The plan for the service continuity process details how the organization will perform service continuity planning, including the development of service continuity plans. Service continuity plans are service-specific plans for sustaining services and associated assets under degraded conditions. Subpractice • Define and document the plan for performing the process. • Define and document the process description. • Review the plan with relevant stakeholders and get their agreement. • Revise the plan as necessary.	

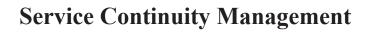| Q2	**CERT-RMM Reference**	
	Consider sponsoring policies and procedures for service continuity management. Such standards should include : • methods for identifying and prioritizing high-value services • methods for analyzing service dependencies and interdependencies • templates for developing and documenting service continuity plans • methods, techniques, and tools for performing consistent and structured version control and for managing changes to service continuity plans • tools for archiving, storing, and securing service continuity plans • tools for providing access control over service continuity plan inquiries, modifications, and deletions • tools for managing the service continuity plan inventory/database, including controlling access and managing changes • methods for communicating with stakeholders (Refer to the Communications process area.) • methods for distributing up-to-date versions of service continuity plans to stakeholders • methods for analyzing plan dependencies and resolving conflicts • methods, techniques, and tools for testing plans and documenting results • methods and tools for capturing and maintaining the list of files and databases that constitute vital records (Refer to the Knowledge and Information Management process area.)	
Q3	**CERT-RMM Reference**	
	Consider identifying stakeholders of the service continuity management process. Examples include: • owners of high-value services and supporting assets (for which plans must be developed) • custodians of high-value services and supporting assets (who may need to execute or participate in plans) • organizational unit and line of business managers responsible for high-value services and supporting assets • staff involved in developing plans • external entities on which service continuity plans are dependent, such as public emergency management staff and other public agencies, partners, and suppliers • external entities responsible for managing high-value services • external entities to which the organization is a supplier • regulatory and legal entities to which the organization is required to submit service continuity plans • staff involved in versioning, storing, archiving, and securing plans • staff involved in testing plans • internal and external auditors	

Q4	**CERT-RMM Reference** Consider developing standards and guidelines for service continuity management, including: • planning for the process • making decisions about the process • making commitments to service continuity plans and activities as well as the process plan • developing service continuity plans and the process plan • communicating service continuity plans and activities and process plans and activities • coordinating process activities • participating in the test and execution of service continuity plans • reviewing and appraising the effectiveness of process activities • establishing requirements for the process • resolving issues in the process	
MIL3-Managed		
1.	Is there management oversight of the performance of the service continuity activities?	
2.	Have qualified staff been assigned to perform service continuity activities as planned?	
3.	Is there adequate funding to perform service continuity activities as planned?	
4.	Are risks related to the performance of planned service continuity activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the service continuity management process. Periodic reviews are needed to ensure that • the process is a planned and coordinated activity • process planning is driven by managing and mitigating organizational risk • internal and external dependencies that affect the process and service continuity plans are identified and considered • vital organizational records are identified • all service continuity plans have assigned owners • service continuity plans are developed, resourced, and validated for high-value services, including new services that are developed and acquired • service continuity plans are tested when developed and periodically as dictated by business conditions and the need to manage risk • changes to service continuity plans and the plan inventory/database are controlled • access to service continuity plans is limited to authorized staff • the effectiveness of service continuity plans is measured • the process is improved based on testing and experience in executing plans • status reports are provided to appropriate stakeholders in a timely manner • process issues are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • actions resulting from internal and external audits are being closed in a timely manner	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in the skills necessary to perform service continuity management. Such skills include: • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop service continuity plans and programs, including the process plan • knowledge required to develop service continuity plans • communication skills for conveying the contents of service continuity plans to stakeholders • knowledge unique to each type of service that is required to develop service-specific continuity plans • knowledge necessary to work effectively with service and asset owners and custodians • knowledge necessary to plan and conduct service continuity testing • knowledge of the tools, techniques, and methods necessary to perform the process using the selected methods, techniques, and tools	
Q3	**CERT-RMM Reference** Consider ensuring that service continuity management activities are adequately funded. Funding the process should extend beyond the initial development of service continuity management activities, tools, and processes to ensure that the organization maintains a capability to ensure the resilience of essential services.	

Q4	**CERT-RMM Reference** Consider managing risk from the failure of the service continuity management process. Failures can occur in: • planning for the process • making decisions about the process • making commitments to service continuity plans and activities as well as the process plan • developing service continuity plans and the process plan • communicating service continuity plans and activities and process plans and activities • coordinating process activities • participating in the test and execution of service continuity plans • reviewing and appraising the effectiveness of process activities • establishing requirements for the process • resolving issues in the process	
MIL4-Measured		
1.	Are service continuity activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are service continuity activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of service continuity?	

Option(s) for Consideration:	

Q1	**CERT-RMM Reference**
	Consider measuring the service continuity management process. Examples of measures include:
	• number and percentage of service continuity plans
	  - completed
	  - tested, and number of times tested by time period
	  - executed, and number of times executed by event on date
	  - that have never been executed
	• number of service continuity plans that have not yet been developed (percentage of high-value services
	  and supporting assets that do not have service continuity plans)
	• percentage of plans
	  - without established owners
	  - that require changes
	  - with missing components (assigned owner, resources, etc.)
	  - that exhibit dependencies on other plans
	  - that exhibit one or more conflicts (such as a single point of failure)
	  - that have not been tested
	  - that have failed one or more test objectives
	  - that have failed in execution
	  - that have not been reviewed post-execution
	  - that have been changed without authorization, review, or testing
	• frequency of changes to plans by service or service type
	• percentage of plan test objectives (RTOs and RPOs) unmet
	• number of plans without identified stakeholders
	• percentage of staff who have not been trained on their roles and responsibilities as defined in
	  service continuity plans
	• number of process risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank)
	• level of adherence to process policies; number of policy violations; number of policy exceptions
	  requested and number approved
	• number of process activities that are on track per plan
	• rate of change of resource needs to support the process
	• rate of change of costs to support the process	

Q2	**CERT-RMM Reference** Consider objectively evaluating the service continuity process, to ensure that: • the process is a planned and coordinated activity • process planning is driven by managing and mitigating organizational risk • internal and external dependencies that affect the process and service continuity plans are identified and considered • vital organizational records are identified • all service continuity plans have assigned owners • service continuity plans are developed, resourced, and validated for high-value services, including new services that are developed and acquired • service continuity plans are tested when developed and periodically as dictated by business conditions and the need to manage risk • changes to service continuity plans and the plan inventory/database are controlled • access to service continuity plans is limited to authorized staff • the effectiveness of service continuity plans is measured • the process is improved based on testing and experience in executing plans • status reports are provided to appropriate stakeholders in a timely manner • process issues are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • actions resulting from internal and external audits are being closed in a timely manner	
Q3	**CERT-RMM Reference** Consider ensuring that the organization Reviews the activities, status, and results of the service continuity management process with higher-level managers and resolves issues.	
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?	
2.	Are improvements to service continuity documented and shared across the organization?	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to service continuity management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting service continuity management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Service Continuity Management

7 Risk Management

MIL-1					MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

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]	
2.	Have categories been established for risks? [RISK: SG1.SP1]	
3.	Has a plan for managing operational risk been established? [RISK: SG1.SP2]	
4.	Is the plan for managing operational risk communicated to stakeholders? [RISK: SG1.SP2]	

	Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[RISK: SG1.SP1]** Determine operational risk sources. 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. Risk sources represent 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 Advance definition of specific risk sources for the organization provides a means for early identification of risk and can seed mitigation plans that can cover a broad array of operational risks before the organization realizes the consequences of these risks. **Additional References** Special Publication 800-37 Revision 1"Guide for Applying the Risk Management Framework to Federal Information Systems" Page 6-8	
Q2	**CERT-RMM Reference** **[RISK: SG1.SP1]** Determine operational risk categories.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. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 7-9	

Q3	**CERT-RMM Reference** **[RISK: SG1.SP2]** Develop and document an operational risk management strategy that aligns with the organization's overall enterprise risk management strategy. Because of the pervasive nature of operational risk, a comprehensive operational risk management strategy is needed to ensure proper consideration of risk and the effects on operational resilience. The strategy provides a common foundation for the performance of operational risk management activities and for the collection, coordination, and elevation of operational risk to the organization's risk management process. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 7-9	
Q4	**CERT-RMM Reference** **[RISK: SG1.SP2]** Communicate the operational risk management strategy to relevant stakeholders and obtain their commitment to the activities. The strategy should be documented and communicated to all relevant stakeholders, internal and external, who are responsible for any operational risk management activity. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 9-11	
Goal 2 – Risk tolerances are identified, and focus of risk management is established.		
1.	Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK: SG2.SP2]	
2.	Have impact areas been prioritized to determine their relative importance? [RISK: SG2.SP2]	
3.	Have risk tolerance parameters been established for each impact area? [RISK: SG2.SP2]	
4.	Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK: SG2.SP1]	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[RISK: SG2.SP2]** Define organizational impact areas. Organizational impact areas identify the 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. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 9-11 "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" Page Entire Document	
Q2	**CERT-RMM Reference** **[RISK: SG2.SP2]** Prioritize areas of impact for the organization. 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. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 37-40	
Q3	**CERT-RMM Reference** **[RISK: SG2.SP2]** Define and document risk measurement and evaluation criteria. 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. The range of criteria can be either qualitative (high, medium, low) or quantitative (based on levels of loss, fines, number of customers lost, etc.). **Additional References** FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems Page 2 "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" Page 32-33	
Q4	**CERT-RMM References** **[RISK: SG2.SP1]** Define risk thresholds for each risk category. 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.	

	Additional References Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 11	
Goal 3 – Risks are identified.		
1.	Are operational risks that could affect delivery of the critical service identified? [RISK: SG3.SP2]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[RISK:SG3.SP2]** Identify the services that are associated with each asset-specific risk statement. Update the risk statement to reflect associated services. Examining risk in the context of services provides the organization additional information that must be considered when prioritizing risks for disposition and mitigation. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process"	
Goal 4 – Risks are analyzed and assigned a disposition.		
1.	Are risks analyzed to determine potential impact to the critical service NQ4 [RISK: SG4.SP1]?	
2.	Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK: SG4.SP3]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[RISK:SG4.SP1]** Evaluate the identified risks using the defined risk parameters and risk measurement criteria. 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 weigh 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. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process"	
Q2	**CERT-RMM Reference** **[RISK: SG4.SP3]** Assign a risk disposition to each risk statement based on risk valuation and prioritization and obtain approval for the proposed disposition of each risk, particularly risks that are not going to be mitigated. 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. Risks that are to be accepted must be approved by a sufficient level of organizational management that accepts responsibility and authority for the potential impact on operational resilience that could result. Risks that are to be transferred must demonstrate a clear and willing party (organization or person) able to accept the risk. Risks that are to be researched or deferred must be carefully examined to ensure that delaying mitigation will not result in the realization of the risk or effects on operationalresilience. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Appendix I"Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process" Page 58-64	

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]	
2.	Are identified risks tracked to closure? [RISK: SG5.SP2]	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[RISK: SG5.SP1]** Develop risk mitigation plans for all risks that have a "mitigation" or "control" disposition. 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 have 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 **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Section 3	
Q2	**CERT-RMM Reference** **[RISK: SG5.SP2]** Provide a method for tracking open risks to closure. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 19-36	
MIL2-Planned	
1.	Is there a documented plan for performing risk management activities?	
2.	Is there s documented policy for risk management?	
3.	Have stakeholders for risk management activities have identified and made aware of their roles?	
4.	Have risk management activities standards and guidelines been identified and implemented?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider developing a plan for risk management process. The plan for the risk management process should be directly influenced by the strategic and operational planning processes of the organization and reflect strategic objectives and initiatives where appropriate. The plan for the risk management process should not be confused with a risk management plan or plans for mitigating risk as the plan for the risk management process details how the organization will perform risk management, including the development of risk management and mitigation plans.	

Q2	**CERT-RMM Reference**
	Consider establishing a risk management policy that addresses
	• responsibility, authority, and ownership for performing process activities
	• procedures, standards, and guidelines for
	  - identifying risk sources and categories of risk
	  - defining risk parameters (such as risk tolerance thresholds) and risk measurement criteria
	  - assigning risk priorities based on risk valuation
	  - assigning risk dispositions
	  - developing risk mitigation plans
	• periodically monitoring the status of all risks and adjusting as necessary
	• methods for measuring adherence to policy, exceptions granted, and policy violations	

Q3	**CERT-RMM Reference** Consider identifying stakeholders of the risk management process. These are examples of stakeholders: • organizational unit managers, line of business managers, project managers, and business process owners • owners of identified assets and services (for which plans to manage risks must be developed) • custodians of identified assets and services (who may need to execute or participate in plans) • staff involved in identifying, analyzing, mitigating, and controlling risks to assets and services (such as information technology, human resources, legal, and compliance staff) • staff involved in reviewing and adjusting strategies to protect and sustain assets and services • the owner of any resilience management process who has referred risks to the process • risk owners • risk mitigation plan owners	
Q4	**CERT-RMM Reference** Consider developing standards and guidelines that address • identifying risk sources and categories of risk • defining risk parameters (such as risk tolerance thresholds) and risk measurement criteria • assigning risk priorities based on risk valuation • assigning risk dispositions • developing risk mitigation plans	

MIL3-Managed		
1.	Is there management oversight of the performance of the risk management activities?	
2.	Have qualified staff been assigned to perform risk management activities as planned?	
3.	Is there adequate funding to perform risk management activities as planned?	
4.	Are risks related to the performance of planned risk management activities identified, analyzed, disposed of, monitored, and controlled?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider measuring the risk management process. These are examples of metrics for the risk management process: • percentage of identified assets and services for which some form of risk assessment has been performed and documented as required by policy • percentage of identified assets and services for which the impact or cost of compromise has been quantified • percentage of identified risks that do not have a defined risk disposition • percentage of identified risks that have a defined mitigation plan against which status is reported in accordance with policy • percentage of identified risks that have not been tracked to closure • change in volume of risks that have been identified over a selected period • percentage of previously identified risks that have converted to a risk disposition of "mitigate" • percentage of identified assets for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters and risk measurement criteria • percentage of identified services for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters and risk measurement criteria • percentage of security incidents that caused damage, compromise, or loss to identified assets or services beyond established risk parameters and risk measurement criteria • percentage of realized risks that have exceeded established risk thresholds • percentage of identified or realized risks that have been characterized as "high" impact according to the organization's risk evaluation criteria • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	

Q2	**CERT-RMM Reference** Consider assigning qualified staff to perform risk management processes. These are examples of staff required to perform the risk management process: • organizational unit managers, line of business managers, project managers, and asset and service owners and custodians. • the chief risk officer or equivalent • a risk management steering council, group, or process group • staff responsible for - identifying operational risk sources and categories - identifying and assessing operational risks, including risks identified by the process and other resilience management processes - business impact analysis - scenario planning and analysis - assigning risk disposition to risk statements based on risk valuation and prioritization - developing risk mitigation plans and implementing these plans, including accepting, deferring, or transferring residual risk - monitoring and tracking risks to closure - managing external entities that have contractual obligations for risk management activities • higher-level managers responsible for defining risk parameters, including risk tolerance thresholds, authorization for levels of risk acceptance, organizational impact areas and priorities, and risk measurement criteria • staff skilled in interview techniques and the use of questionnaires and surveys • vital managers and subject matter experts • external entities involved in process activities and in assessing risk on outsourced functions • internal and external auditors responsible for reporting to appropriate committees on process effectiveness	
Q3	**CERT-RMM Reference** Consider ensuring that risk management activities are adequately funded. Funding considerations should include ensuring that risk is adequately identified, assessed, and mitigated on a continuous basis, and that risk management activities are not treated as discrete occasional activities.	
Q4	**CERT-RMM Reference** Consider identifying risk to the organization that arises from failed risk management processes. Deviations from the risk management plan may occur because operational risks for assets and services vary widely, and thus the mitigation of these risks may require process deviations. The organization must determine if the deviations are appropriate given the risk parameters and whether the deviation will result in an impact on operational resilience.In addition, deviations from the risk management plan may occur when organizational units fail to follow the enterprise-sponsored process. These deviations may affect the operational resilience of the organizational unit's services but may also have a cascading effect on enterprise operational resilience objectives.	

MIL4-Measured	
1.	Are risk management activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are risk management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of risk management?	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider measuring risk management activities to ensure their effectiveness. These are examples of metrics for the risk management process: • percentage of identified assets and services for which some form of risk assessment has been performed and documented as required by policy • percentage of identified assets and services for which the impact or cost of compromise has been quantified • percentage of identified risks that do not have a defined risk disposition • percentage of identified risks that have a defined mitigation plan against which status is reported in accordance with policy • percentage of identified risks that have not been tracked to closure • change in volume of risks that have been identified over a selected period • percentage of previously identified risks that have converted to a risk disposition of "mitigate" • percentage of identified assets for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters and risk measurement criteria • percentage of identified services for which a mitigation plan has been implemented to mitigate risks as necessary and to maintain these risks within acceptable risk parameters and risk measurement criteria • percentage of security incidents that caused damage, compromise, or loss to identified assets or services beyond established risk parameters and risk measurement criteria • percentage of realized risks that have exceeded established risk thresholds • percentage of identified or realized risks that have been characterized as "high" impact according to the organization's risk evaluation criteria • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	

Q2	**CERT-RMM Reference** Consider reviewing activities, status, and results of the process with the immediate level of managers responsible for the process and identify issues. Reviews of the risk management process may result from periodic examination or post-event audits that seek to identify problems that must be corrected. Elevating the results of these examinations to managers provides an opportunity to correct process deficiencies and to make managers aware of variations in the risk management process that not only have localized impact but may also affect the organization's resilience as a whole.	
Q3	Consider objectively evaluating adherence of the risk management process against its process description, standards, and procedures, and address non-compliance.	
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?	
2.	Are improvements to risk management documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing and tailoring process assets, including standard processes. Subpractice: • Select from the organization's set of standard processes those processes that cover the risk management process and best meet the needs of the organizational unit or line of business. • Establish the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensure that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Document the defined process and the records of the tailoring. • Revise the description of the defined process as necessary.	

| Q2 | **CERT-RMM Reference** Collect risk management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets. These are examples of improvement work products and information:
• metrics and measurements of the viability of the process
• changes and trends in operating conditions that affect risk sources and categories
• changes in risk conditions and the risk environment that affect risk parameters, measurement criteria, or
   risk dispositions
• lessons learned in post-event review of continuity exercises, incidents, and disruptions in continuity, particularly those that result in losses or compromises that exceed risk parameters and measurement
   criteria
• process lessons learned that can be applied to improve operational resilience management performance
   and internal controls
• issues with the risk identification, analysis, prioritization, overall assessment, mitigation, and monitoring
   processes
• lessons learned from both successfully and unsuccessfully mitigating identified risks
• risk mitigation plan costs and benefits for future return on investment analysis
• resilience requirements that are not being satisfied or are being exceeded | |

Other Observations – Risk Management

8   External Dependency Management

MIL-1					MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	G4	G5	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

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]	
2. Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1]	
3. Are external dependencies prioritized? [EXD:SG1.SP2]	
Option(s) for Consideration:	
Q1 **CERT-RMM Reference** **[EXD:SG1.SP1]** Identify External Dependencies. It is important for the organization to identify and characterize all such external dependencies so that they can be understood, formalized, monitored, and managed as part of the organization's comprehensive risk management process. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page E-2	
Q2 **CERT-RMM Reference** **[EXD:SG1.SP1]**Establish a process for creating and maintaining the list of external dependencies and entities. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 19	

Q3	**CERT-RMM Reference** **[EXD:SG1.SP2]** Apply the prioritization criteria to the list of external dependencies to produce a prioritized list. Depending on the prioritization scheme developed by the organization, the result might be several lists, tiers, or sets of external dependencies. Be sure that external dependencies that are required for the successful execution of security activities, service continuity plans, and service restoration plans are prioritized appropriately. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 25-26	
Goal 2 – Risks due to external dependencies are identified and managed.		
1.	Are risks due to external dependencies identified and managed? [EXD:SG2.SP1]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[EXD:SG2.SP1]** Identify risks due to external dependencies. Identification of risks due to external dependencies requires an understanding of the actions of the associated external entity in the operation, support, or resilience of the organization's services. External entities will be responsible for varying dependencies in the support of the organization's operations. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Appendix D	
Goal 3 – Relationships with external entities formally established and maintained.		
1.	Have resilience requirements of the critical service been established that apply specifically to each external dependency? [EXD:SG3.SP2]	
2.	Are these requirements reviewed and updated? [EXD:SG3.SP2]	
3.	Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	
4.	Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[EXD:SG3.SP2]** For each external dependency, establish a list of resilience specifications that apply to the responsible external entity. The process for determining and documenting the resilience specifications that apply to an external dependency and entity will vary based on the action of the entity in relation to the organization's operations and the priority of the external dependency. At a minimum, the resilience specifications should include a clear and definitive statement of the external entity's services, support, products, assets, or staff on which the organization relies. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 24-26	
Q2	**CERT-RMM Reference** **[EXD:SG3.SP2]** Periodically review and update resilience specifications for external dependencies and entities as conditions warrant	
Q3	**CERT-RMM Reference** **[EXD:SG3.SP3]** Evaluate external entities based on their abilities to meet the resilience specifications and in accordance with the established selection criteria. **Additional References** Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" Page 24-26	
Q4	**CERT-RMM Reference** **[EXD:SG3.SP4]** Properly document the agreement terms, conditions, specifications and other provisions. All agreement provisions should be documented in the agreement in language that is unambiguous. The agreement should not contain any general exceptions for achieving the resilience specifications unless they are carefully considered and negotiated. It may, however, contain scenarios of types of unforeseen events for which the external entity is not expected to prepare. Any exceptions granted to resilience specifications or scenarios for which the external entity is not required to prepare should be treated as risks. All agreements should establish and enable procedures for monitoring the performance of external entities and inspecting the services or products they deliver to the organization. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" SA-4	
Goal 4 – Performance of external entities is managed.		
1.	Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1]	
2.	Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1]	

3.	Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	
4.	Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[EXD:SG4.SP1]** Establish procedures and responsibility for monitoring external entity performance and inspecting any external entity deliverables. Procedures should be consistent with the agreement between the organization and the external entity and should be based on verifying that the external entity is achieving the specifications as defined in the agreement. All agreement specifications should be considered for monitoring; it may be appropriate to prioritize monitoring and inspection activities based on a risk analysis of the specifications (which includes all external dependencies). Monitoring and inspection procedures should address the external entity's required characteristics, required behaviors, and required performance parameters.	
Q2	**CERT-RMM Reference** **[EXD:SG4.SP1]** Establish the responsibility for monitoring external entity performance and inspecting any external entity deliverables. (Responsibility is typically assigned to the organizational owner of the relationship.) **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" SA-9	
Q3	**CERT-RMM Reference** **[EXD:SG4.SP2]** The agreement should be reviewed to identify appropriate and allowable corrective actions for consideration. The various alternatives should be evaluated based on their likelihood to succeed in correcting the situation and mitigating any associated risks. It may be valuable and appropriate to include the external entity in the discussion and consideration of alternatives, especially if both the organization and the external entity desire to continue the relationship. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" SA-12	
Q4	**CERT-RMM Reference** **[EXD:SG4.SP2]** Monitor as appropriate to ensure that issues are remedied in a timely manner. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" SA-13	

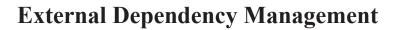| Goal 5 – Dependencies on public services and infrastructure service providers are identified.	
1.	Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	
2.	Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[EC:SG4.SP3]** Identify and document public services on which facilities rely. Typically, this activity results from business impact analysis. However, it can be included as part of service continuity planning or facility asset definition, depending on the organization. A resulting list of public services for each facility should be documented and made available for inclusion in service continuity plans as appropriate. **Additional References** Special Publication 800-34 "Contingency Planning for Federal Information Systems" Page 53,55	
Q2	**CERT-RMM Reference** **[EC:SG4.SP4]** Identify and document internal infrastructure dependencies that the organization relies upon to provide services. Remember that these dependencies may be internal as well as external, particularly where the organization has control over certain aspects of facility infrastructure such as power or telecommunications that they provide for their own operations. Typically, this activity results from business impact analysis. However, it can be included as part of service continuity planning or facility asset definition, depending on the organization. A resulting list of public infrastructure providers for each facility should be documented and made available for inclusion in service continuity plans as appropriate. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-2	
MIL2-Planned	
1.	Is there a documented plan for performing external dependency management activities?	
2.	Is there a documented policy for external dependency management?	
3.	Have stakeholders for external dependency management activities been identified and made aware of their roles?	
4.	Have external dependency management activities standards and guidelines been identified and implemented?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider developing a plan for external dependency management. A plan for performing the external dependencies management process is developed to ensure that the organization can satisfy its operational resilience requirements when an external entity has access to, control of, ownership in, possession of, responsibility for (including development, operations, maintenance, or support), or other defined obligations related to one or more assets or services of the organization. The plan must address the enterprise and resilience specifications for the service being performed or the product being provided (i.e., the external dependency) by the external entity. In addition, because external entities can be located in many geographical locations, the plan must address those external entities and stakeholders that can enable or adversely affect operational resilience.The plan for the external dependencies management process should not be confused with service continuity (recovery, restoration) plans for assets and services that are under the control of external entities. The plan for the external dependencies management process details how the organization will manage external dependencies and relationships with external entities, including the development of service continuity plans where such entities are involved. Subpractice: • Define and document the plan for performing the process. • Define and document the process description. • Review the plan with relevant stakeholders and get their agreement. • Revise the plan as necessary.	

| Q2 | **CERT-RMM Reference**
Consider developing policies and procedures for external dependency management. The external dependencies management policy should address
• responsibility, authority, and ownership for performing process activities
• procedures, standards, and guidelines for - identifying and prioritizing external dependencies
- associating external dependencies with services and assets
- managing operational risks resulting from external dependencies
- evaluating and selecting external entities
- formalizing and enforcing agreements with external entities, including changing any provisions by mutual agreement
- developing and documenting enterprise and resilience specifications for external entities, including organizational policies to which external entities are expected to adhere
• standards of performance and service levels
• establishing service continuity plans and procedures for external entities
• monitoring the performance of external entities, including inspecting the services or products they deliver (Such procedures specify frequency, protocol, and responsibility for monitoring and inspection.)
• terminating relationships with external entities as specified in formal agreements
• issue escalation and dispute resolution
• requesting, approving, providing, and terminating access for external entities
• methods for measuring adherence to policy, exceptions granted, and policy violations | |
| Q3 | **CERT-RMM Reference**
Consider identifying stakeholders of the external dependency management process. Examples include:
• internal and external owners and custodians of organizational assets
• internal and external service owners
• organizational unit and line of business managers responsible for high-value assets and the services they support
• staff responsible for managing operational risks arising from external dependencies and relationships with external entities
• staff responsible for establishing, implementing, and maintaining an internal control system for   organizational assets where an external dependency and an external entity are involved
• staff required to develop, test, implement, and execute service continuity plans that involve external dependencies and external entities
• acquisition and procurement staff
• internal and external auditors | |

Q4	**CERT-RMM Reference** Consider developing standards and guidelines for external dependency management. Include: • list of external dependencies, with priorities • criteria for prioritizing external dependencies • affinity analyses results to inform dependency prioritization and risk identification • information that defines external dependencies, stored as a maintainable information repository or database • risk statements with impact valuation • list of external dependency risks with categorization and prioritization, risk disposition, mitigation plans, and current status • agreement templates, including enterprise specifications that apply to external entities • external dependencies and resilience specifications that apply to each external entity • RFPs, including applicable SLAs • criteria for selecting external entities • proposal evaluation results and decision rationale • agreements with external entities, including contracts, memoranda of agreement, purchase orders, and licensing agreements • performance-monitoring reports • relationship management databases • inspection reports on deliverables • corrective-action reports • process plan • policies and procedures	
MIL3-Managed		
1.	Is there management oversight of the performance of the external dependency management activities?	
2.	Have qualified staff been assigned to perform external dependency management activities as planned?	
3.	Is there adequate funding to perform external dependency management activities as planned?	
4.	Are risks related to the performance of external dependency management activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the external dependency management process. Ensure the organization: • definite roles and responsibilities in the process plan • includes process tasks and responsibility for these tasks in specific job descriptions • develops policy requiring organizational unit managers, line of business managers, project managers, and asset and service owners and custodians to participate in the process for services and assets under their ownership or custodianship • develops and implementing agreements, including contracts, SLAs, memoranda of agreement, purchase orders, and licensing agreements • includes process tasks in staff performance management goals and objectives, with requisite measurement of progress against these goals	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in skills required in external dependency management. These are examples of skills required in the organizational training and awareness process: • identifying and prioritizing external dependencies • affinity analyses • elicitation of resilience specifications to be reflected in RFPs and agreements with external entities • evaluating and selecting external entities • negotiating agreements with external entities • prioritizing external entities based on the priority of the external dependencies for which the entity is responsible • knowledge of tools, techniques, and methods that can be used to identify, analyze, mitigate, and monitor operational risks resulting from external dependencies and from relationships with external entities • managing relationships with external entities • monitoring the performance of external entities, including the inspection of deliverables and knowing when corrective actions are called for	
Q3	**CERT-RMM Reference** Consider ensuring that external dependency management activities are adequately funded. Funding the process should extend beyond the initial development of the activities, but include maintenance and refresh.	

Q4	**CERT-RMM Reference** Consider managing risk arising from insufficient external dependency management practices. Examples of practices that might be evaluated include: • list of external dependencies, with priorities • criteria for prioritizing external dependencies • affinity analyses results to inform dependency prioritization and risk identification • information that defines external dependencies, stored as a maintainable information repository or database • risk statements with impact valuation • list of external dependency risks with categorization and prioritization, risk disposition, mitigation plans, and current status • agreement templates, including enterprise specifications that apply to external entities • external dependencies and resilience specifications that apply to each external entity • RFPs, including applicable SLAs • criteria for selecting external entities • proposal evaluation results and decision rationale • agreements with external entities, including contracts, memoranda of agreement, purchase orders, and licensing agreements • performance-monitoring reports • relationship management databases • inspection reports on deliverables • corrective-action reports • process plan • policies and procedures	
MIL4-Measured		
1.	Are external dependency management activities periodically reviewed and measured to ensure they are effective and producing intended results.	
2.	Are external dependency management activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to external dependency management?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider measuring the adherence of the external dependency management process against its process description, standards, and procedures, and address non-compliance. • number and percentage of external entities in a variety of categories, such as - by external dependency - by business process, by service, by asset or product - by type of service or product provided - by prioritized tier (based on prioritization criteria) - by agreement type (formal contract with and without SLA, memorandum of agreement, purchase order, licensing agreement, and other, including no type of agreement) - by number or type of agreement changes - by status (RFP, source selection, awarded, contract initiated, performing as expected, out of compliance, in dispute or litigation, terminated, renewed, etc.) - by monetary value - by geographic region - by operational throughput that relies upon the external entity (for example, number of customers, transaction volume) - by number of entities external to itself upon which the external entity relies to meet its agreements with the organization - by CERT-RMM capability rating • percentage of external dependencies without designated organizational owners • percentage of external entities without designated organizational owners • percentage of external entities whose financial status is at risk • percentage of external entities that have undergone some form of assessment, risk assessment, and audit as required by policy • percentage of external entities that - play a key role in fulfilling service continuity plans during disruptive events - have tested their service continuity plans, including their participation in the organization's service continuity plans per agreement - failed to perform as expected during a disruptive event • percentage of external entities whose deliverables have failed to pass inspection • percentage of external entities with corrective actions that have not been remedied in the designated time period • number of external dependency risks referred to the risk management process; number of risks where corrective action is still pending (by risk rank) • level of adherence to process policies; number of policy violations; number of policy exceptions requested and number approved • number of process activities that are on track per plan • rate of change of resource needs to support the process • rate of change of costs to support the process	
Q2	**CERT-RMM Reference** Consider objectively evaluating adherence of the external dependency management process against its process description, standards, and procedures, and address non-compliance.	

Q3	**CERT-RMM Reference** Consider ensuring that the organization reviews the activities, status, and results of the external dependency management process with higher-level managers and resolves issues.	
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?	
2.	Are improvements to external dependency management documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to external dependency management, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting external dependency management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – External Dependencies Management

9   Training and Awareness

MIL-1		MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

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]	
2.	Have required cyber security skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP2]	
3.	Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1]	
4.	Have cyber security training needs been identified? [OTA:SG3.SP1]	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** **[OTA:SG1.SP1]** Analyze the organization's operational resilience program to identify the types and extent of awareness efforts that are necessary to satisfy resilience program objectives. Because managing operational resilience requires acculturation of both internal and external parties (staff), the types and extent of awareness efforts may need to be extensive and rigorous. The objectives of awareness efforts must be clearly stated and must help the organization achieve inculcation of staff to the organization's philosophy of managing operational resilience. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	
Q2	**CERT-RMM Reference** **[HRM:SG1.SP1]** Establish and document baseline competencies necessary to meet the needs of the organization's operational resilience management process. 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.) and position (CIO, senior security analyst, network engineer, etc.). **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	

Q3	**CERT-RMM Reference** **[OTA:SG3.SP1]** Collect information about skill gaps, cross-training, and succession planning by reviewing the job responsibilities of staff involved in resilience processes, as well as current performance levels. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model" Section 5	
Q4	**CERT-RMM Reference** **[OTA:SG3.SP1]** Document the resilience training needs of the organization. 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. The training needs should also adequately cover the capabilities represented by the operational resilience management process. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	
Goal 2 – Awareness and training activities are conducted.		
1.	Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1]	
2.	Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1]	
3.	Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	
4.	Are awareness and training activities revised as needed? [OTA:SG1.SP3 and OTA:SG3.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[OTA:SG2.SP1]** Perform awareness activities according to the schedule and the plan. Awareness materials are distributed to the target populations according to the schedule and the approaches established in the plan. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	

Q2	**CERT-RMM Reference** **[OTA:SG4.SP1]** Conduct the training.Experienced instructors should perform training. When possible, training is conducted in settings that closely resemble actual performance conditions and includes activities to simulate actual work situations. This approach includes integration of tools, methods, and procedures for competency development. 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. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	
Q3	**CERT-RMM Reference** **[OTA:SG2.SP3, OTA:SG4.SP3]** Provide a mechanism for evaluating the effectiveness of each awareness activity with respect to the objectives for that activity. For awareness presentations, this mechanism should include evaluations of the material and the presenters. Provide a mechanism for assessing the effectiveness of each training course with respect to established organizational, project, or individual learning (or performance) objectives. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model" Section 7.3.2	
Q4	**CERT-RMM Reference** **[OTA:SG1.SP3, OTA:SG3.SP3]** Revise the awareness materials and supporting artifacts as necessary. Revise the resilience training needs of the organization as necessary. **Additional References** Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model" Section 4.1	

MIL2-Planned		
1.	Is there a documented plan for performing training activities?	
2.	Is there a documented policy for training?	
3.	Have stakeholders for training activities been identified and made aware of their roles?	
4.	Have training standards and guidelines been identified and implemented?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider developing a plan for training and awareness. • Special consideration in the plan may have to be given to training and awareness for skill development, sustaining skill competencies, and reassignment planning for various roles. These activities aid in protecting and sustaining people to support operational resilience. • Special consideration in the plan may also have to be given to how the organization incorporates training and awareness activities for resources that are not under its direct control, including external entities such as contractors, outsourcing partners, training suppliers, and other business partners. • Define and document the process description. • Review the plan with relevant stakeholders and get their agreement. • Revise the plan as necessary.	
Q2	**CERT-RMM Reference** Consider developing policies and procedures for training and awareness. Include the following: • methods and tools for building and distributing awareness messages, including pens, mugs, posters, signage, screen savers, newsletters, etc. • instruments for analyzing training needs • training workstations and other hardware needs • instructional design tools • packages for developing presentation materials • tools, methods, and procedures that closely resemble actual performance conditions and simulate actual work situations • methods for delivering awareness and training materials, from user on-demand training to classroom-based training • tools for tracking awareness and training course attendance and successful and unsuccessful completion by designated staff • methods for evaluating the effectiveness of awareness activities, including surveys, focus groups, interviews, etc. • methods for evaluating the effectiveness of training activities, including testing, assessment mechanisms, etc. • tools used to capture and securely store training records and ensure such records are accessed only by authorized staff	

Q3	**CERT-RMM Reference** Consider identifying stakeholders of the training and awareness process. Examples include: • staff who are required to determine the degree to which their constituencies understand the organization's resilience goals, objectives, standards, policies, and processes, including: - asset owners and custodians - service owners - business process owners - organizational unit and line of business managers responsible for high-value services and assets • external entities responsible for managing high-value assets and services • human resources (for ensuring the resilience of people assets) • information technology staff (for ensuring the resilience of technology assets) • staff responsible for physical security (for ensuring the resilience of facility assets) • internal and external auditors	
Q4	**CERT-RMM Reference** Consider developing standards and guidelines for training and awareness. Include: • awareness and training needs • awareness and training plans and programs • awareness and training records and waivers • awareness and training materials and supporting work products • instructor evaluation forms • awareness and training effectiveness surveys • survey and interview results • awareness and training examinations and assessment results • policies and procedures • contracts with external entities	
MIL3-Managed		
1.	Is there management oversight of the performance of the training activities?	
2.	Have qualified staff been assigned to perform training activities as planned?	
3.	Is there adequate funding to perform training activities as planned?	
4.	Are risks related to the performance of planned training activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the training and awareness process as needed to ensure control over: • awareness and training needs • awareness and training plans and programs • awareness and training records and waivers • awareness and training materials and supporting work products • instructor evaluation forms • awareness and training effectiveness surveys • survey and interview results • awareness and training examinations and assessment results • policies and procedures • contracts with external entities	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in skills required in training and awareness. These are examples of skills required in the organizational training and awareness process: • curriculum and instructional design • course delivery • course and instructor evaluation • measuring the effectiveness of awareness and training materials • structuring and conducting participant surveys and interviews • knowledge of the tools, techniques, and methods necessary to create, deliver, and maintain training and awareness work products, including those necessary to perform the process using the selected methods, techniques, and tools • knowledge unique to each operational resilience management process area and assets and services that are the focus of these processes • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop effective process requirements, plans, and programs	
Q3	**CERT-RMM Reference** Consider ensuring that training and awareness activities are adequately funded. Funding the process should extend beyond the initial development of the training and awareness programs, but include maintenance and refresh.	
Q4	**CERT-RMM Reference** Consider managing risk arising from insufficient training and awareness practices. Examples of practices that might be evaluated include: • awareness and training needs • awareness and training plans and programs • awareness and training records and waivers • awareness and training materials and supporting work products • instructor evaluation forms • awareness and training effectiveness surveys • survey and interview results • awareness and training examinations and assessment results • policies and procedures • contracts with external entities	

MIL4-Measured	
1.	Are training activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are training activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to the performance of training?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider measuring the adherence of the training and awareness activities against their process description, standards, and procedures, and address non-compliance.	
Q2	**CERT-RMM Reference** Consider objectively evaluating adherence of the training and awareness processes against their process description, standards, and procedures, and address non-compliance.	
Q3	**CERT-RMM Reference** Consider ensuring that the organization Reviews the activities, status, and results of the training and awareness process with higher-level managers and resolves issues.	
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?	
2.	Are improvements to training documented and shared across the organization?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to training and awareness, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting training and awareness work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Training and Awareness

10   Situational Awareness

MIL-1			MIL-2				MIL-3				MIL-4			MIL-5	
G1	G2	G3	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

Goal 1 – Threat monitoring is performed.		
1.	Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]	
2.	Have threat monitoring procedures been implemented? [MON:SG2.SP2]	
3.	Have resources been assigned to threat monitoring processes? [MON:SG2.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[MON:SG1.SP2]** Identify stakeholders of the monitoring process. The list should include internal and external stakeholders and should be seeded by examining operational resilience management processes and their organizational owners. Stakeholders of the organization's monitoring processes are those internal and external people, entities, or agencies that require information about the operational resilience management processes for which they have responsibility and for which they must achieve resilience goals, objectives, and obligations. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 7-10	
Q2	**CERT-RMM Reference** **[MON:SG2.SP2]** Review, refine, and develop monitoring operating procedures. Detailed processes, standard operating procedures, or work instructions may be created during monitoring infrastructure implementation, but they will need to be regularly reviewed, tailored, and possibly supplemented to meet ongoing monitoring needs. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 19-26	

Q3	**CERT-RMM Reference** **[MON:SG2.SP3]** Assign resources to monitoring processes. Ensure that monitoring support staff have received appropriate training to perform the necessary monitoring activities. These are examples of training: • operating, monitoring, and configuring monitoring systems components • supporting stakeholders in understanding and interpreting monitoring data • securing data collected from monitoring systems components **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" Page 16-17	
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]	
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]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[COMM:SG1.SP1]** Identify relevant stakeholders that may have a vested interest or vital role in communications about resilience. When determining which stakeholders to include in the list, consider • rationale for stakeholder involvement • roles and responsibilities of the relevant stakeholders • relationships between stakeholders • relative importance of the stakeholder to success of the program • resources (e.g., training, materials, time, and funding) needed to ensure stakeholder interaction. Stakeholders and their communications needs may be defined as a part of other operational resilience management processes. For example, the communication needs of staff involved in the incident management process may be defined by that process. These communications requirements should be considered independently of the processes and practices in the Communications process area because they have a specialized purpose and involve specific stakeholders. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations" Page 22-23	

Q2	**CERT-RMM Reference** **[COMM:SG1.SP1]** Establish a plan that describes the involvement of all communications stakeholders. The plan identifies all internal and external stakeholders, including their roles and classes, as well as the types, frequencies, and levels of communication they are to receive in specified circumstances. **Additional References** Special Publication 800-137 "Information Security Continuous Monitoring for Federal Information Systems and Organizations" Page 22-24	
Goal 3 – Threat information is communicated.		
1.	Is threat information communicated to stakeholders? [COMM:SG3.SP2]	
2.	Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	
3.	Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** **[COMM:SG3.SP2]** Communicate threat information to stakeholders. Implement and manage communications infrastructure. From a generic standpoint, the organization's communications infrastructure must support communications requirements from stakeholders. **Additional References** Special Publication 800-30 "Risk Management Guide for Information Technology Systems" Page 14-15	
Q2	**CERT-RMM Reference** **[COMM:SG2.SP3]** Assign resources to communications processes roles and responsibilities. Staff are assigned authority and accountability for carrying out the communications plan and program. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-3	
Q3	**CERT-RMM Reference** **[COMM:SG2.SP3]** Ensure that organizational training is provided to communications staff respective to the specific resilience communications role they perform. This is especially important for communications roles in other operational resilience management processes such as incident management and in the execution of service continuity plans. **Additional References** Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations" CP-3	
MIL2-Planned		
1.	Is there a documented plan for performing situational awareness activities?	

2.	Is there a documented policy for situational awareness?	
3.	Have stakeholders for situational awareness activities been identified and made aware of their roles?	
4.	Have situational awareness standards and guidelines been identified and implemented?	
Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider developing a plan for situational awareness. Special consideration in the plan may have to be given to information acquisition, sustaining skill competencies, and planning for changes in the operating environment. These activities aid in protecting and sustaining critical services. Special consideration in the plan may also have to be given to how the organization validates and communicates about cyber security information, and how the organization will maintain a common operating picture.	
Q2	**CERT-RMM Reference** Consider developing policies and procedures for situational awareness. Include the following: • methods and tools for rapidly learning cyber security information, • processes that will enable effective analysis of cyber security information • criteria that might be used to evaluate sources of cyber security information. • identification of methods of communicating cyber security information across the organization to enable a common operating picture • repositories of cyber security information • Possible actions that the organization might take in an effort to temporarily reduce its attack surface in the event of inclement cyber security information.	

Q3	**CERT-RMM Reference** Consider identifying stakeholders of the situational awareness process. Examples include: • owners of high-value services and supporting assets (for which plans must be developed) • custodians of high-value services and supporting assets (who may need to execute or participate in plans) • organizational unit and line of business managers responsible for high-value services and supporting assets • staff involved in developing plans • external entities on which service continuity plans are dependent, such as public emergency management staff and other public agencies, partners, and suppliers • external entities responsible for managing high-value services • external entities to which the organization is a supplier • regulatory and legal entities to which the organization is required to submit service continuity plans • staff involved in versioning, storing, archiving, and securing plans • staff involved in testing plans • internal and external auditors	
Q4	**CERT-RMM Reference** Consider sponsoring standards, and guidelines, including procedures, standards, and guidelines for • monitoring cyber security information • recording relevant cyber security information • evaluating sources of cyber security information • communicating cyber security information • reducing the organization's attack surface • methods for measuring adherence to policy, exceptions granted, and policy violations.	
MIL3-Managed		
1.	Is there management oversight of the performance of situational awareness activities?	
2.	Have qualified staff been assigned to perform situational awareness activities as planned?	
3.	Is there adequate funding to perform situational awareness activities as planned?	
4.	Are risks related to the performance of planned situational awareness activities identified, analyzed, disposed of, monitored, and controlled?	

Option(s) for Consideration:		
Q1	**CERT-RMM Reference** Consider conducting periodic reviews of the situational awareness process as needed to ensure that: • the process is a planned and coordinated activity • process planning is driven by managing and mitigating organizational risk • internal and external dependencies that affect the process and service continuity plans are identified and considered • the effectiveness of situational awareness plans is measured • the process is improved based on testing and experience in executing plans • status reports are provided to appropriate stakeholders in a timely manner • process issues are referred to the risk management process when necessary • actions requiring management involvement are elevated in a timely manner • the performance of process activities is being monitored and regularly reported • key measures are within acceptable ranges as demonstrated in governance dashboards or scorecards and financial reports • actions resulting from internal and external audits are being closed in a timely manner	
Q2	**CERT-RMM Reference** Consider ensuring that responsible staff are trained in the skills necessary to perform situational awareness. Such skills include: • knowledge necessary to elicit and prioritize stakeholder requirements and needs and interpret them to develop situational awareness plans and programs, including the process plan • knowledge required to identify relevant sources of cyber security information • communication skills for conveying the contents of situational awareness plans to stakeholders • knowledge required to identify methods to establish a common operating picture • knowledge required to identify methods of reducing the organization's attack surface in response to a hostile environment.	
Q3	**CERT-RMM Reference** Consider ensuring that situational awareness activities are adequately funded .Funding the process should extend beyond the initial development of situational awareness activities, tools, and processes to ensure that the organization maintains a capability to ensure the resilience of essential services.	
Q4	**CERT-RMM Reference** Consider managing risk from the failure of the situational awareness process. Failures can occur in: • planning for the process • making decisions about the process • making commitments to plans and activities as well as the process plan • effective communication about cyber security • development of a common operating picture • development of effective plans to reduce the organization's attack surface.	

MIL4-Measured	
1.	Are situational awareness activities periodically reviewed and measured to ensure they are effective and producing intended results?	
2.	Are situational awareness activities periodically reviewed to ensure they are adhering to the plan?	
3.	Is higher-level management aware of issues related to situational awareness?	
Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider measuring the situational awareness process against its process description, standards, and procedures, and address non-compliance. Examples of measurement include: • number of sources of cyber security evaluated for trustworthiness • percentage of stakeholders who receive cyber security information within the defined thresholds • percentage of services that have attack surface reduction plans • number of stakeholders who seek situational awareness information out on a daily basis.	
Q2	**CERT-RMM Reference** Consider objectively evaluating adherence of the situational awareness process against its process description, standards, and procedures, and address non-compliance.	
Q3	**CERT-RMM Reference** Consider ensuring that the organization Reviews the activities, status, and results of the situational awareness process with higher-level managers and resolves issues.	
MIL5-Defined	
1.	Has the organization adopted a standard definition of the situational awareness activities from which operating units can derive practices that fit their unique operating circumstances?	
2.	Are improvements to situational awareness activities documented and shared across the organization?	

Option(s) for Consideration:	
Q1	**CERT-RMM Reference** Consider establishing an organization-wide approach to situational awareness, that includes: • Selecting from the organization's set of standard processes those processes that cover the asset definition and management process and best meet the needs of the organizational unit or line of business. • Establishing the defined process by tailoring the selected processes according to the organization's tailoring guidelines. • Ensuring that the organization's process objectives are appropriately addressed in the defined process, and ensure that process governance extends to the tailored processes. • Documenting the defined process and the records of the tailoring. • Revising the description of the defined process as necessary.	
Q2	**CERT-RMM Reference** Consider collecting situational awareness work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement of the organization's processes and process assets.	

Other Observations – Situational Awareness

List of Resources Referenced in this Report

Resource Name	URL
"A Complete Guide to the Common Vulnerability Scoring System Version 2.0"	http://www.first.org/cvss/cvss-guide.pdf
"Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process"	http://www.cert.org/archive/pdf/07tr012.pdf
CERT Resilience Management Model (CERT®-RMM)	http://www.cert.org/resiliency/rmm.html
Draft Special Publication 800-16 Revision 1 "Information Security Training Requirements: A Role-and Performance-Based Model"	http://csrc.nist.gov/publications/drafts/800-16-rev1/draft_sp800_16_rev1_2nd-draft.pdf
FIPS Publication 199 Standards for Security Categorization of Federal Information and Information Systems	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
FIPS Publication 200 "Minimum Security Requirements for Federal information and information Systems"	http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
Handbook for Computer Security Incident Response Teams (CSIRTs)	http://www.cert.org/archive/pdf/csirt-handbook.pdf
Managing for Enterprise Security	http://www.cert.org/archive/pdf/managinges0412.pdf
Special Publication 800-18 Revision 1 "Guide for Developing Security Plans for Federal Information Systems"	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
Special Publication 800-30 "Risk Management Guide for Information Technology Systems"	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
Special Publication 800-34 "Contingency Planning for Federal Information Systems"	http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
Special Publication 800-37 Revision 1"Guide for Applying the Risk Management Framework to Federal Information Systems"	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
Special Publication 800-39 "Managing Information Security Risk Organization, Mission, and Information System View"	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
Special Publication 800-40 Version 3.0 "Creating a Patch Management and Vulnerability Management Program"	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
Special Publication 800-53 Revision 4 "Recommended Security Controls for Federal Information Systems and Organizations"	http://dx.doi.org/10.6028/NIST.SP.800-53r4
Special Publication 800-61 "Computer Security Incident Handling guide"	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
Special Publication 800-70 "National Checklist Program for IT Products: Guidelines for Checklist Users and Developers"	http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf
Special Publication 800-84 "Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities"	http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf
Special Publication 800-128 "Guide for Security Configuration Management of Information Systems"	http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
Special Publication 800-137 "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"	http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

Contact Information for Questions Related to this Report

For any questions regarding the CRR Self-Assessment please email **cse@hq.dhs.gov**.