



Copyright 2024 Carnegie Mellon University. All Rights Reserved.

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

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

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

External Use: Additionally, this material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Permission can be requested at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

[DISTRIBUTION STATEMENT F] Further dissemination only as directed by Department of Defense Cyber Crime Center, DCISE@dc3.mil (determination date: 2019-03-20) or higher DoD authority.

DM19-0303

# CYBER RESILIENCE ANALYSIS

## Contents

<b>CMMC 2.0 to Cyber Resilience Analysis (CRA) Crosswalk</b>	<b>1</b>
Access Control (AC)	2
Audit and Accountability (AU)	3
Awareness and Training (AT)	4
Configuration Management (CM)	4
Identification and Authentication (IA)	5
Incident Response (IR)	6
Maintenance (MA)	6
Media Protection (MP)	7
Personnel Security (PS)	7
Physical Protection (PE)	8
Risk Assessment (RA)	8
Security Assessment (CA)	8
System and Communications Protection (SC)	9
System and Information Integrity (SI)	10
Crosswalk Reference Key	11
 <b>Cyber Resilience Analysis (CRA) to CMMC 2.0 Crosswalk</b>	 <b>12</b>
1 Asset Management	13
2 Controls Management	21
3 Configuration and Change Management	26
4 Vulnerability Management	29
5 Incident Management	33
6 Service Continuity Management	37
7 Risk Management	40
8 External Dependencies Management	43
9 Training and Awareness	46
10 Situational Awareness	48
Crosswalk Reference Key	50

# CYBER RESILIENCE **ANALYSIS**

## CMMC 2.0 to Cyber Resilience Analysis (CRA) Crosswalk

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
Access Control (AC)						
AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	3.1.1	AC-2 AC-3 AC-17	AM:G2.Q1-PT AM:G2.Q5 AM:G5.Q1 – ITF† AM:G5.Q2 – ITF	AM:G5.Q3 – ITF AM:G5.Q4 – ITF EDM:G1.Q1 EDM:G1.Q2	
AC.L1-3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	3.1.2	AC-2 AC-3 AC-17	AM:G5.Q1 – ITF AM:G5.Q2 – ITF	AM:G5.Q3 – ITF AM:G5.Q4 – ITF	
AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.	3.1.3	AC-4	AM:G2.Q5 CM:G2.Q3	CM:G2.Q4 CM:G2.Q5	
AC.L2-3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	3.1.4	AC-5	AM:G5.Q6 – ITF		
AC.L2-3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3.1.5	AC-6 AC-6(1) AC-6(5)	AM:G5.Q5 – ITF		
AC.L2-3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	3.1.6	AC-6(2)	AM:G5.Q5 – ITF		
AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	3.1.7	AC-6(9) AC-6(10)	AM:G5.Q3 – ITF AM:G5.Q4 – ITF AM:G5.Q5 – ITF CCM:G2.Q2		
AC.L2-3.1.8	Limit unsuccessful logon attempts.	3.1.8	AC-7	CM:G2.Q1		
AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	3.1.9	AC-8	AM:G6.Q3		
AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	3.1.10	AC-11 AC-11(1)	CM:G2.Q1		
AC.L2-3.1.11	Terminate (automatically) user sessions after a defined condition.	3.1.11	AC-12	CM:G2.Q1		
AC.L2-3.1.12	Monitor and control remote access sessions.	3.1.12	AC-17(1)	VM:G1.Q5		
AC.L2-3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	3.1.13	AC-17(2)	CM:G2.Q4 CM:G2.Q5		
AC.L2-3.1.14	Route remote access via managed access control points.	3.1.14	AC-17(3)	CM:G2.Q2 CM:G2.Q8		
AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	3.1.15	AC-17(4)	AM:G5.Q1 – ITF AM:G5.Q2 – ITF	AM:G5.Q3 – ITF AM:G5.Q4 – ITF	
AC.L2-3.1.16	Authorize wireless access prior to allowing such connections.	3.1.16	AC-18	CM:G2.Q8		
AC.L2-3.1.17	Protect wireless access using authentication and encryption.	3.1.17	AC-18(1)	CM:G2.Q4 CM:G2.Q8		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

† Denotes CRA reference with format of [CRA Domain:Goal.Question-Asset type(s) (PITF)].



# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
AC.L2-3.1.18	Control connection of mobile devices.	3.1.18	AC-19	CM:G2.Q6 CM:G2.Q8 CM:G2.Q10	VM:G1.Q3 VM:G1.Q4 VM:G1.Q5	
AC.L2-3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	3.1.19	AC-19(5)	CM:G2.Q3 CM:G2.Q5		
AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	3.1.20	AC-20 AC-20(1)	AM:G2.Q1 – T AM:G2.Q5 AM:G6.Q3 CM:G2.Q8 EDM:G1.Q1 EDM:G1.Q2 EDM:G1.Q3 EDM:G3.Q1 EDM:G3.Q2	EDM:G3.Q3 EDM:G3.Q4 EDM:G4.Q1 EDM:G4.Q2 EDM:G4.Q3 EDM:G4.Q4 EDM:G5.Q1 EDM:G5.Q2	
AC.L2-3.1.21	Limit use of portable storage devices on external systems.	3.1.21	AC-20(2)	CM:G2.Q7		
AC.L1-3.1.22	Control information posted or processed on publicly accessible information systems.	3.1.22	AC-22	AM:G6.Q3	CM:G2.Q5	
<b>Audit and Accountability (AU)</b>						
AU.L2-3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	3.3.1	AU-2 AU-3 AU-3(1) AU-6 AU-11 AU-12	CM:G2.Q6		
AU.L2-3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3.3.2	AU-2 AU-3 AU-3(1) AU-6 AU-11 AU-12	AM:G5.Q7		
AU.L2-3.3.3	Review and update logged events.	3.3.3	AU-2(3)	CM:G2.Q6 IM:G2.Q1 IM:G2.Q2 IM:G2.Q3 IM:G2.Q4	IM:G2.Q5 IM:G2.Q7 IM:G2.Q8 IM:G2.Q9	
AU.L2-3.3.4	Alert in the event of an audit logging process failure.	3.3.4	AU-5	IM:G2.Q1		
AU.L2-3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	3.3.7	AU-8 AU-8(1)	CM:G2.Q6		
AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	3.3.5	AU-6(3)	IM:G2.Q1 IM:G2.Q2 IM:G2.Q3	IM:G2.Q4 IM:G2.Q5 IM:G3.Q3	
AU.L2-3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	3.3.6	AU-7	CM:G2.Q6		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	3.3.8	AU-9	AM:G5.Q1 CM:G2.Q6		
AU.L2-3.3.9	Limit management of audit logging functionality to a subset of privileged users.	3.3.9	AU-9(4)	AM:G5.Q6 – ITF		
<b>Awareness and Training (AT)</b>						
AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	3.2.1	AT-2 AT-3	AM:MIL2.Q2 CM:MIL2.Q2 CCM:MIL2.Q2 VM:MIL2.Q2 IM:MIL2.Q2 SCM:MIL2.Q2 EDM:MIL2.Q2 RM:G3.Q1 RM:MIL2.Q2	TA:G1.Q1 TA:G2.Q1 TA:G2.Q2 TA:G2.Q3 TA:G2.Q4 TA:G2.Q5 TA:G2.Q6 TA:G2.Q7 TA:MIL2.Q2 SA:MIL2.Q2	
AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	3.2.2	AT-2 AT-3	AM:G6.Q4 AM:MIL2.Q3 AM:MIL3.Q2 CM:MIL2.Q3 CM:MIL3.Q2 CCM:MIL2.Q3 CCM:MIL3.Q2 VM:MIL2.Q3 VM:MIL3.Q2 IM:MIL2.Q3 IM:MIL3.Q2 SCM:MIL2.Q3 SCM:MIL3.Q2 EDM:MIL2.Q3 EDM:MIL3.Q2 RM:MIL2.Q3 RM:MIL3.Q2	TA:G1.Q2 TA:G1.Q3 TA:G1.Q4 TA:G2.Q2 TA:G2.Q3 TA:G2.Q4 TA:G2.Q5 TA:G2.Q6 TA:G2.Q7 TA:MIL2.Q3 TA:MIL3.Q2 SA:G1.Q3 SA:G3.Q3 SA:MIL2.Q3 SA:MIL3.Q2	
AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	3.2.3	AT-2(2)	TA:G1.Q1 TA:G2.Q1	TA:G2.Q3 TA:G2.Q4	
<b>Configuration Management (CM)</b>						
CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	3.4.1	CM-2 CM-6 CM-8 CM-8(1)	AM:G2.Q1 – PITF AM:G2.Q2 – PITF AM:G2.Q3 – PITF AM:G2.Q4 – PITF AM:G2.Q5 AM:G3.Q1 – PITF AM:G3.Q2 – PITF AM:G4.Q1 – PITF AM:G4.Q2 – PITF	CCM:G1.Q6 CCM:G2.Q1 CCM:G3.Q1 CCM:G3.Q2 CCM:G3.Q3 CCM:G3.Q4 CCM:G3.Q5 CCM:G3.Q6	
CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	3.4.2	CM-2 CM-6 CM-8 CM-8(1)	CCM:G2.Q1 CCM:G2.Q2 CCM:G2.Q3 CCM:G3.Q1		
CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.	3.4.3	CM-3	CCM:G1.Q1 – ITF CCM:G1.Q4 CCM:G1.Q5	CCM:G2.Q3 CCM:G2.Q5 CCM:G2.Q6 CCM:G2.Q7	

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.	3.4.4	CM-4	CCM:G1.Q2 – ITF	CCM:G2.Q3 CCM:G2.Q7	
CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	3.4.5	CM-5	AM:G5.Q1 – ITF AM:G5.Q2 – ITF AM:G5.Q3 – ITF AM:G5.Q4 – ITF	CCM:G2.Q4 CCM:G2.Q8	
CM.L2-3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	3.4.6	CM-7	CM:G2.Q10		
CM.L2-3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	3.4.7	CM-7(1) CM-7(2)	CM:G2.Q10		
CM.L2-3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	3.4.8	CM-7(4) CM-7(5)	CM:G2.Q10		
CM.L2-3.4.9	Control and monitor user-installed software.	3.4.9	CM-11	VM:G1.Q5		
<b>Identification and Authentication (IA)</b>						
IA.L1-3.5.1	Identify information system users, processes acting on behalf of users, or devices.	3.5.1	IA-2 IA-3 IA-5	AM:G1.Q1 AM:G2.Q1-PT AM:G2.Q5 AM:G5.Q7	EDM:G1.Q1 EDM:G1.Q2	
IA.L1-3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	3.5.2	IA-2 IA-3 IA-5	AM:G2.Q1-T AM:G5.Q1 – ITF AM:G5.Q2 – ITF AM:G5.Q3 – ITF	AM:G5.Q4 – ITF AM:G5.Q7 EDM:G1.Q1 EDM:G1.Q2	
IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	3.5.3	IA-2(1) IA-2(2) IA-2(3)	CM:G2.Q1		
IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	3.5.4	IA-2(8) IA-2(9)	CM:G2.Q1		
IA.L2-3.5.5	Prevent the reuse of identifiers for a defined period.	3.5.5	IA-4	CM:G2.Q1		
IA.L2-3.5.6	Disable identifiers after a defined period of inactivity.	3.5.6	IA-4	CM:G2.Q1		
IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	3.5.7	IA-5(1)	CM:G2.Q1		
IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.	3.5.8	IA-5(1)	CM:G2.Q1		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.



# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	3.5.9	IA-5(1)	CM:G2.Q1		
IA.L2-3.5.10	Store and transmit only cryptographically-protected passwords.	3.5.10	IA-5(1)	CM:G2.Q1		
IA.L2-3.5.11	Obscure feedback of authentication information.	3.5.11	IA-6	CM:G2.Q1		
<b>Incident Response (IR)</b>						
IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	3.6.1	IR-2 IR-4 IR-5 IR-6 IR-7	IM:G1.Q1 IM:G1.Q2 IM:G1.Q3 IM:G1.Q4 IM:G2.Q1 IM:G2.Q2 IM:G2.Q3 IM:G2.Q4 IM:G2.Q5 IM:G2.Q8 IM:G2.Q9 IM:G3.Q2 IM:G4.Q2 IM:G5.Q1	IM:G5.Q2 IM:G5.Q3 SCM:G1.Q1 – PITF SCM:G1.Q2 SCM:G1.Q3 SCM:G1.Q4 SCM:G1.Q5 SCM:G1.Q6 SCM:G1.Q7 SCM:G2.Q1 SCM:G4.Q1 SCM:G4.Q2 SCM:G4.Q3	
IR.L2-3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	3.6.2	IR-2 IR-4 IR-5 IR-6 IR-7	IM:G2.Q1 IM:G2.Q2 IM:G2.Q3 IM:G2.Q4 IM:G2.Q5 IM:G2.Q6 IM:G2.Q7	IM:G2.Q9 IM:G3.Q1 IM:G3.Q2 IM:G3.Q3 IM:G4.Q1 IM:G4.Q2 IM:G4.Q3 IM:G4.Q4	
IR.L2-3.6.3	Test the organizational incident response capability.	3.6.3	IR-3	IM:G1.Q2 SCM:G3.Q1 SCM:G3.Q2	SCM:G3.Q3 SCM:G3.Q4 SCM:G3.Q5	
<b>Maintenance (MA)</b>						
MA.L2-3.7.1	Perform maintenance on organizational systems.	3.7.1	MA-2 MA-3 MA-3(1) MA-3(2)	CCM:G2.Q9 CCM:G2.Q11		
MA.L2-3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	3.7.2	MA-2 MA-3 MA-3(1) MA-3(2)	CCM:G2.Q10 CCM:G2.Q11 CCM:MIL3.Q2		
MA.L2-3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	3.7.3	MA-2	AM:G6.Q6 AM:G6.Q7		
MA.L2-3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3.7.4	MA-3(2)	CCM:G2.Q10 VM:G1.Q3		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
MA.L2-3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	3.7.5	MA-4	CCM:G2.Q11		
MA.L2-3.7.6	Supervise the maintenance activities of personnel without required access authorization.	3.7.6	MA-5	CCM:G2.Q9 CCM.G2.Q11		
Media Protection (MP)						
MP.L2-3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3.8.1	MP-2 MP-4 MP-6	AM:G6.Q3 CM:G2.Q3 CM:G2.Q5 CM:G2.Q7		
MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	3.8.2	MP-2 MP-4 MP-6	AM:G5.Q1 – ITF AM:G5.Q2 – ITF AM:G5.Q3 – ITF	AM:G5.Q4 – ITF CM:G2.Q7	
MP.L1-3.8.3	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	3.8.3	MP-2 MP-4 MP-6	AM:G6.Q6 AM:G6.Q7		
MP.L2-3.8.4	Mark media with necessary CUI markings and distribution limitations.	3.8.4	MP-3	AM:G6.Q1 AM:G6.Q2 AM:G6.Q3		
MP.L2-3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	3.8.5	MP-5	AM:G5.Q1 AM:G6.Q3 CM:G2.Q3 CM:G2.Q7		
MP.L2-3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	3.8.6	MP-5(4)	CM:G2.Q3 CM:G2.Q5 CM:G2.Q7		
MP.L2-3.8.7	Control the use of removable media on system components.	3.8.7	MP-7	CM:G2.Q7		
MP.L2-3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3.8.8	MP-7(1)	CM:G2.Q7		
MP.L2-3.8.9	Protect the confidentiality of backup CUI at storage locations.	3.8.9	CP-9	AM:G6.Q3 AM:G6.Q5		
Personnel Security (PS)						
PS.L2-3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3.9.1	PS-3 PS-4 PS-5	CM:G2.Q9		
PS.L2-3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	3.9.2	PS-3 PS-4 PS-5	AM:G5.Q3 AM:G5.Q4 CM:G2.Q9		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
Physical Protection (PE)						
PE.L1-3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	3.10.1	PE-2 PE-4 PE-5 PE-6	AM:G5.Q1 – ITF AM:G5.Q2 – ITF	AM:G5.Q3 – ITF AM:G5.Q4 – ITF	
PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	3.10.2	PE-2 PE-4 PE-5 PE-6	CM:G2.Q5 VM:G1.Q5		
PE.L1-3.10.3	Escort visitors and monitor visitor activity.	3.10.3	PE-3	VM:G1.Q5		
PE.L1-3.10.4	Maintain audit logs of physical access.	3.10.4	PE-3	CM:G2.Q6		
PE.L1-3.10.5	Control and manage physical access devices.	3.10.5	PE-3	CM:Q2.Q1		
PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	3.10.6	PE-17	AM:G6.Q3		
Risk Assessment (RA)						
RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	3.11.1	RA-3	RM:G1.Q1 RM:G1.Q2 RM:G1.Q3 RM:G1.Q4 RM:G2.Q1 RM:G2.Q2 RM:G2.Q3	RM:G2.Q4 RM:G3.Q1 RM:G4.Q1 RM:G4.Q2 RM:G5.Q1 RM:G5.Q2 EDM:G2.Q1	
RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	3.11.2	RA-5 RA-5(5)	VM:G1.Q1 - PITF VM:G1.Q2 – PITF VM:G2.Q1 – ITF VM:G2.Q2 - ITF VM:G2.Q3 - ITF VM:G2.Q6 - ITF		
RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	3.11.3	RA-5	VM:G2.Q3 - ITF VM:G2.Q4 – ITF VM:G2.Q5 – ITF VM:G2.Q6 – ITF	VM:G3.Q1 VM:G3.Q2 VM:G3.Q3 VM:G4.Q1	
Security Assessment (CA)						
CA.L2-3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	3.12.1	CA-2 CA-5 CA-7 PL-2	CM:G3.Q1 – PITF CM:G4.Q1 – PITF		
CA.L2-3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3.12.2	CA-2 CA-5 CA-7 PL-2	CM:G3.Q2 CM:G4.Q1 CM:G4.Q2 VM:G3.Q1	VM:G3.Q2 VM:G3.Q3 VM:G4.Q1	

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description	NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
CA.L2-3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	3.12.3	CA-2 CA-5 CA-7 PL-2	CM:G3.Q1 – PITF CM:G4.Q1 – PITF		
CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	3.12.4	CA-2 CA-5 CA-7 PL-2	AM:G2.Q2 – PITF AM:G2.Q5 AM:G3.Q1 – PITF AM:G3.Q2 – PITF AM:G7.Q1 AM:G7.Q2	AM:G7.Q3 CM:G1.Q1 – PITF CM:G1.Q2 CCM:G1.Q3 VM:G1.Q1 – PITF	
<b>System and Communications Protection (SC)</b>					
SC.L1-3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	3.13.1	SC-7 SA-8	AM:G2.Q5 CM:G2.Q2 CM:G2.Q4	CM:G2.Q5 CM:G2.Q8	
SC.L2-3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	3.13.2	SC-7 SA-8	AM:G2.Q2 – PITF AM:G3.Q2 – PITF CM:G1.Q1 – PITF	CM:G1.Q2 CM:G2.Q1 CCM:G1.Q6	
SC.L2-3.13.3 Separate user functionality from system management functionality.	3.13.3	SC-2	AM:G5.Q5 – ITF CM:G2.Q10		
SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	3.13.4	SC-4	AM:G5.Q1 – ITF AM:G5.Q2 – ITF AM:G5.Q3 – ITF	AM:G5.Q4 – ITF AM:G5.Q5 – ITF	
SC.L1-3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	3.13.5	SC-7	CM:G2.Q2		
SC.L2-3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	3.13.6	SC-7(5)	CM:G2.Q2		
SC.L2-3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	3.13.7	SC-7(7)	CM:G2.Q2 CM:G2.Q8		
SC.L2-3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3.13.8	SC-8 SC-8(1)	CM:G2.Q3 CM:G2.Q4 CM:G2.Q5		
SC.L2-3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	3.13.9	SC-10	CM:G2.Q1		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

CMMC 2.0 Practice and Description		NIST 800 171 Relevant Control	NIST 800 53 Relevant Controls	CRA Mapping*		Comments
SC.L2-3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	3.13.10	SC-12	CM:G2.Q3 CM:G2.Q4		
SC.L2-3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3.13.11	SC-13	CM:G2.Q3 CM:G2.Q4		
SC.L2-3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	3.13.12	SC-15	CM:G2.Q8		
SC.L2-3.13.13	Control and monitor the use of mobile code.	3.13.13	SC-18	VM:G1.Q4		
SC.L2-3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	3.13.14	SC-19	CM:G2.Q8		
SC.L2-3.13.15	Protect the authenticity of communications sessions.	3.13.15	SC-23	CM:G2.Q4		
SC.L2-3.13.16	Protect the confidentiality of CUI at rest.	3.13.16	SC-28	CM:G2.Q3		
<b>System and Information Integrity (SI)</b>						
SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	3.14.1	SI-2 SI-3 SI-5	VM:G2.Q1 – ITF VM:G2.Q2 – ITF VM:G2.Q3 – ITF VM:G2.Q5 – ITF VM:G2.Q6 – ITF	VM:G3.Q1 VM:G3.Q2 VM:G3.Q3 VM:G4.Q1	
SI.L1-3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	3.14.2	SI-2 SI-3 SI-5	VM:G1.Q3		
SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	3.14.3	SI-2 SI-3 SI-5	VM:G2.Q1 – ITF VM:G2.Q2 – ITF IM:G2.Q2 IM:G2.Q4 IM:G2.Q5 IM:G2.Q7 IM:G4.Q2	SA:G1.Q1 SA:G1.Q2 SA:G1.Q3 SA:G2.Q1 SA:G2.Q2 SA:G3.Q1 SA:G3.Q2 SA:G3.Q3	
SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.	3.14.4	SI-3	VM:G1.Q3		
SI.L1-3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	3.14.5	SI-3	VM:G1.Q3 VM:G1.Q4 VM:G1.Q5		
SI.L2-3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	3.14.6	SI-4 SI-4(4)	VM:G1.Q5 IM:G2.Q1		
SI.L2-3.14.7	Identify unauthorized use of organizational systems.	3.14.7	SI-4	VM:G1.Q5 IM:G2.Q1		

\* RMM references for the CRA questions can be found in the CRA to CMMC Level 1 through Level 3 Crosswalk starting on page 12.

# CYBER RESILIENCE ANALYSIS

## Crosswalk Reference Key

Cyber Resilience Analysis (CRA) Reference Key	
<b>AM</b>	Asset Management
<b>CCM</b>	Configuration and Change Management
<b>CM</b>	Controls Management
<b>EDM</b>	External Dependencies Management
<b>IM</b>	Incident Management
<b>RM</b>	Risk Management
<b>SA</b>	Situational Awareness
<b>SCM</b>	Service Continuity Management
<b>TA</b>	Training and Awareness
<b>VM</b>	Vulnerability Management
<b>Gx</b>	Goal
<b>Qx</b>	Question
<b>P</b>	People
<b>I</b>	Information
<b>T</b>	Technology
<b>F</b>	Facilities
<b>MIL</b>	CRA Maturity Indicator Level

<b>RMM</b>	<a href="https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084">https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084</a>
<b>CMMC</b>	<a href="https://www.acq.osd.mil/cmmc/">https://www.acq.osd.mil/cmmc/</a>

Cybersecurity Maturity Model Certification (CMMC) Reference Key	
<b>AC</b>	Access Control
<b>AM</b>	Access Management
<b>AU</b>	Audit and Accountability
<b>AT</b>	Awareness and Training
<b>CM</b>	Configuration Management
<b>IA</b>	Identification and Authentication
<b>IR</b>	Incident Response
<b>MA</b>	Maintenance
<b>MP</b>	Media Protection
<b>PS</b>	Personnel Security
<b>PE</b>	Physical Protection
<b>RE</b>	Recovery
<b>RA</b>	Risk Assessment
<b>CA</b>	Security Assessment
<b>SA</b>	Situational Awareness
<b>SC</b>	System and Communications Protection
<b>SI</b>	System and Information Integrity
<b>ML</b>	Process Maturity

† RMM references for the CRA questions can be found in the CRA to CMMC Crosswalk starting on page 12.



# CYBER RESILIENCE **ANALYSIS**

## Cyber Resilience Analysis (CRA) to CMMC 2.0 Crosswalk

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis Practice	CMMC Practice and Description	Notes
	<b>1 Asset Management</b> The purpose of Asset Management is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services.		
	<b>Goal 1—Services are identified and prioritized.</b>		
	1.	Are services identified? [SC:SG2.SP1] <sup>§</sup>	IA.L1-3.5.1 Identify information system users, processes acting on behalf of users, or devices.
	2.	Are services prioritized based on analysis of the potential impact if the services are disrupted? [SC:SG2.SP1]	
	3.	Is the organization's mission, vision, values and purpose, including the organization's place in critical infrastructure, identified and communicated? [EF:SG1.SP1]	
	4.	Are the organization's mission, objectives, and activities prioritized? [EF:SG1.SP3] <sup>¶</sup>	
	<b>Goal 2—Assets are inventoried, and the authority and responsibility for these assets is established.</b>		
	1.	Are the assets that directly support the critical service inventoried (technology includes hardware, software, and external information systems)? [ADM:SG1.SP1] <sup>¶</sup>	
	<i>People</i>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
		AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
		IA.L1-3.5.1 Identify system users, processes acting on behalf of users, and devices.	
	<i>Information</i>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	<i>Technology</i>	AC.L1-3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
		AC.L1-3.1.20 Verify and control/limit connections to and use of external systems.	
		IA.L1-3.5.1 Identify system users, processes acting on behalf of users, and devices.	
		IA.L1-3.5.2. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	
	<i>Facilities</i>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
		CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	

<sup>§</sup> Denotes RMM reference with format of [Process Area: Specific Goal: Specific Practice].

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis Practice	CMMC Practice and Description	Notes
	2. Do asset descriptions include protection and sustainment requirements? [ADM:SG1.SP2]	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
		CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
		SC.L2-3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
		RE.3.139 Regularly perform complete, comprehensive, and resilient data backups as organizationally defined.	
	3. Are both owners and custodians of assets documented in asset descriptions? [ADM:SG1.SP3]	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	4. Are the physical locations of assets (both within and outside the organization) documented in the asset inventory? [ADM:SG1.SP3]	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	5. Are organizational communications and data flows mapped and documented in the asset inventory? [ADM:SG1.SP2]	AC.L1-3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	
		AC.L2-3.1.3 Control the flow of CUI in accordance with approved authorizations.	
		AC.L1-3.1.20 Verify and control/limit connections to and use of external systems.	
		CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
		CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
		IA.L1-3.5.1 Identify system users, processes acting on behalf of users, and devices.	
		SC.L1-3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	

§ Denotes RMM reference with format of [Process Area: Specific Goal.Specific Practice].

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes
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]	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	People	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	Information			
	Technology			
	Facilities			
	Are confidentiality, integrity, and availability requirements established for each service-related asset? [RRD:SG2.SP1]	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	People	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	Information	SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
	Technology			
	Facilities			
Goal 4—The asset inventory is managed.				
1.	Have change criteria been established for asset descriptions? [ADM:SG3.SP1]	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	People			
	Information			
	Technology			
	Facilities			
2.	Are asset descriptions updated when changes to assets occur? [ADM:SG3.SP2]	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	People			
	Information			
	Technology			
	Facilities			

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description			Notes
	Goal 5—Access to assets is managed.				
	1.	Is access (including identities and credentials) to assets granted based on their protection requirements? [AM:SG1.SP1] <sup>¶</sup>	AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
		Information	AC.L1-3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
		Technology	AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	
		Facilities	AU.L2-3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	
			CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
			IA.L1-3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
			MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	
			MP.L2-3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
		PE.L1-3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.		
	SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.			
	2.	Are access (including identities and credentials) requests reviewed and approved by the asset owner? [AM:SG1.SP1] <sup>¶</sup>	AC.L1-3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
		Information	AC.L1-3.1.2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
		Technology	AC.L2-3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	
		Facilities	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
			IA.L1-3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
			MP.L2-3.8.2	Limit access to CUI on system media to authorized users.	
			PE.L1-3.10.1	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	
			SC.L2-3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	3. Are access privileges reviewed to identify excessive or inappropriate privileges? [AM:SG1.SP3] <sup>¶</sup>	AC.L1-3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
		AC.L1-3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
		Information AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
		Technology AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	
		Facilities CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
		IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
		MP.L2-3.8.2 Limit access to CUI on system media to authorized users.	
		PS.L2-3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
	4. Are access privileges modified as a result of reviews? [AM:SG1.SP4]	PE.L1-3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	
		SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	
		AC.L1-3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	
		AC.L1-3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	
		Information AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
		Technology AC.L2-3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	
		Facilities CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
		IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
	5. Are access permissions managed incorporating the principle of least privilege? [AM:SG1.SP1] <sup>¶</sup>	MP.L2-3.8.2 Limit access to CUI on system media to authorized users.	
		PS.L2-3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	
		PE.L1-3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.	
		SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	
		AC.L2-3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	
	6. Are access permissions managed incorporating the principle of separation of duties? [AM:SG1.SP1] <sup>¶</sup>	AC.L2-3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	
		Information AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
		Technology SC.L2-3.13.3 Separate user functionality from system management functionality.	
		Facilities SC.L2-3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	
		AC.L2-3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
		AU.L2-3.3.9 Limit management of audit logging functionality to a subset of privileged users.	
		Information	
		Technology	
		Facilities	

<sup>¶</sup> Denotes a Cyber Hygiene practice.



# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	7. Are identities (e.g., user accounts) proofed before they are bound to credentials that are asserted in interactions? [ID:SG1.SP1] <sup>¶</sup>	AU.L2-3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. IA.L1-3.5.1 Identify information system users, processes acting on behalf of users, or devices. IA.L1-3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	
	<b>Goal 6—Information assets are categorized and managed to ensure the sustainment and protection of the critical service.</b>		
	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] <sup>¶</sup>	MP.L2-3.8.4 Mark media with necessary CUI markings and distribution limitations.	
	2. Is the categorization of information assets monitored and enforced? [KIM:SG1.SP2] <sup>¶</sup>	MP.L2-3.8.4 Mark media with necessary CUI markings and distribution limitations.	
	3. Are there policies and procedures for the proper labeling and handling of information assets? [KIM:SG1.SP2] <sup>¶</sup>	AC.L2-3.1.9 Provide privacy and security notices consistent with applicable CUI rules. AC.L1-3.1.20 Verify and control/limit connections to and use of external information systems. AC.L1-3.1.22 Control information posted or processed on publicly accessible information systems. MP.L2-3.8.2 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. MP.L2-3.8.4 Mark media with necessary CUI markings and distribution limitations. MP.L2-3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations. PE.L2-3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	
	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] <sup>¶</sup>	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	5. Are high-value information assets backed-up and retained? [KIM:SG6.SP1] <sup>¶</sup>	MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations.	
	6. Do guidelines exist for properly disposing of information assets? [KIM:SG4.SP3]	MA.L2-3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. MP.L1-3.8.3 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	
	7. Is adherence to information asset disposal guidelines monitored and enforced? [KIM:SG4.SP3]	MA.L2-3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI. MP.L1-3.8.3 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>Goal 7—Facility assets supporting the critical service are prioritized and managed.</b>		
	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]	CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	2. Is the prioritization of facilities reviewed and validated? [EC:SG1.SP1]	CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	3. Are protection and sustainment requirements of the critical service considered during the selection of facilities? [EC:SG2.SP2]	CA.L2-3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
MIL2-Planned	1. Is there a documented plan for performing asset management activities?		
	2. Is there a documented policy for asset management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for asset management activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have asset management standards and guidelines been identified and implemented?		
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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes
<b>2 Controls Management</b>				
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.				
1.	Have control objectives been established for assets required for delivery of the critical service? [CTRL:SG1.SP1]	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.  Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
	People	SC.L2-3.13.2		
	Information			
	Technology			
	Facilities			
2.	Are control objectives prioritized according to their potential to affect the critical service? [CTRL:SG1.SP1]	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
		SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
Goal 2—Controls are implemented.				
1.	Have controls been implemented to achieve the control objectives established for the critical service? [CTRL:SG2.SP1]	AC.L2-3.1.8	Limit unsuccessful logon attempts.	
		AC.L2-3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	
		AC.L2-3.1.11	Terminate (automatically) user sessions after a defined condition.	
		IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	
		IA.L2-3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	
		IA.L2-3.5.5	Prevent the reuse of identifiers for a defined period.	
		IA.L2-3.5.6	Disable identifiers after a defined period of inactivity.	
		IA.L2-3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	
		IA.L2-3.5.8	Prohibit password reuse for a specified number of generations.	
		IA.L2-3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	
		IA.L2-3.5.10	Store and transmit only cryptographically-protected passwords.	
		IA.L2-3.5.11	Obscure feedback of authentication information.	
		PE.L1-3.10.5	Control and manage physical access devices.	
		SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
		SC.L2-3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	
2.	Have controls been implemented, incorporating network segregation where appropriate, to protect network integrity? [CTRL:SG2.SP1]	AC.L2-3.1.14	Route remote access via managed access control points.	
		SC.L1-3.13.1	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
		SC.L1-3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	
		SC.L2-3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	
		SC.L2-3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	3. Have controls been implemented to protect data-at-rest? [CTRL:SG2.SP1], [KIM:SG4.SP2] <sup>¶</sup>	AC.L2-3.1.3 Control the flow of CUI in accordance with approved authorizations.	
		AC.L2-3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.	
		MP.L2-3.8.2 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
		MP.L2-3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	
		MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
		MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations.	
		SC.L2-3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
		SC.L2-3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	
	4. Have controls been implemented to protect data-in-transit? [CTRL:SG2.SP1], [KIM:SG4.SP1], [KIM:SG4.SP2] <sup>¶</sup>	SC.L2-3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
		SC.L2-3.13.16 Protect the confidentiality of CUI at rest.	
		AC.L2-3.1.3 Control the flow of CUI in accordance with approved authorizations.	
		AC.L2-3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
		AC.L2-3.1.17 Protect wireless access using authentication and encryption.	
		SC.L1-3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
		SC.L2-3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	
	5. Have controls been implemented to protect against data leaks? [CTRL:SG2.SP1], [KIM:SG4.SP1], [KIM:SG4.SP2] <sup>¶</sup>	SC.L2-3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	
		SC.L2-3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	
		SC.L2-3.13.15 Protect the authenticity of communications sessions.	
		AC.L2-3.1.3 Control the flow of CUI in accordance with approved authorizations.	
		AC.L2-3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	
		AC.L2-3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.	
		AC.L1-3.1.22 Control information posted or processed on publicly accessible information systems.	
		MP.L2-3.8.2 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	
		MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	
		MP.L2-3.8.9 Protect the confidentiality of backup CUI at storage locations.	
		PE.L2-3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.	
		SC.L1-3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	
		SC.L2-3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	6. Have audit/log records been determined, documented, implemented, and reviewed in accordance with policy? [CTRL:SG2.SP1], [MON:SG1.SP3] <sup>¶</sup>	AC.L2-3.1.18 Control connection of mobile devices. AU.L2-3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity. AU.L2-3.3.3 Review and update logged events. AU.L2-3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting. AU.L2-3.3.7 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. AU.L2-3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion. PE.L1-3.10.4 Maintain audit logs of physical access.	
	7. Have controls been implemented to protect and restrict the use of removable media in accordance with policy? [CTRL:SG2.SP1], [TM:SG2.SP2] <sup>¶</sup>	AC.L2-3.1.21 Limit use of portable storage devices on external systems. MP.L2-3.8.2 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. MP.L2-3.8.2 Limit access to CUI on system media to authorized users. MP.L2-3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. MP.L2-3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. MP.L2-3.8.7 Control the use of removable media on system components. MP.L2-3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.	
	8. Have controls been implemented to protect communication and control networks? [CTRL:SG2.SP1], [TM:SG2.SP2] <sup>¶</sup>	AC.L2-3.1.14 Route remote access via managed access control points. AC.L2-3.1.16 Authorize wireless access prior to allowing such connections. AC.L2-3.1.17 Protect wireless access using authentication and encryption. AC.L2-3.1.18 Control connection of mobile devices. AC.L1-3.1.20. Verify and control/limit connections to and use of external systems. SC.L1-3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. SC.L2-3.13.2 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. SC.L2-3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling). SC.L2-3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	
	9. Have cybersecurity human resource practices been implemented for the critical service (e.g., de-provisioning, personnel screening)? [CTRL:SG2.SP1], [HRM:SG3.SP1]	PS.L2-3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI. PS.L2-3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.



# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	10. Is access to systems and assets controlled by incorporating the principle of least functionality (e.g., whitelisting, blacklisting, etc.)? [CTRL:SG2.SP1], [TM:SG2.SP2] <sup>¶</sup>	AC.L2-3.1.18 Control connection of mobile devices. CM.L2-3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. CM.L2-3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. CM.L2-3.4.8 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. SC.L2-3.13.3 Separate user functionality from system management functionality.	
	<b>Goal 3—Control designs are analyzed to ensure they satisfy control objectives.</b>		
	1. Are control designs analyzed to identify gaps where control objectives are not adequately satisfied? [CTRL:SG3.SP1]	CA.L2-3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. CA.L2-3.12.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	
	People	CM.L2-3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	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]	CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	<b>Goal 4—The internal control system is assessed to ensure control objectives are met.</b>		
	1. Is the performance of controls assessed on a scheduled basis to verify they continue to meet control objectives? [CTRL:SG4.SP1]	CA.L2-3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	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]	CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
MIL2-Planned	1. Is there a plan for performing controls management activities?		
	2. Is there a documented policy for controls management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for controls management activities have been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have controls management standards and guidelines been identified and implemented?		

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?	AT.L2-3.2.2    Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes	
	<b>3 Configuration and Change Management</b>				
	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.				
	1.	Is a change management process used to manage modifications to assets? [ADM:SG3.SP2]	CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.	
		Information			
		Technology			
		Facilities			
	2.	Are resilience requirements evaluated as a result of changes to assets? [RRM:SG1.SP3]	CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.	
		Information			
		Technology			
		Facilities			
	3.	Is capacity management and planning performed for assets? [TM:SG5.SP3]	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
	4.	Are change requests tracked to closure? [TM:SG4.SP3] <sup>¶</sup>	CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.	
	5.	Are stakeholders notified when they are affected by changes to assets? [ADM:SG3.SP2]	CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.	
	6.	Is a System Development Life Cycle implemented to manage systems supporting the critical service? [ADM:SG3.SP2], [RTSE:SG2.SP2]	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
			SC.L2-3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
	Goal 2—The integrity of technology and information assets is managed.				
	1.	Is configuration management performed for technology assets? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
			CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	2.	Are techniques in use to detect changes to technology assets? [TM:SG4.SP3] <sup>¶</sup>	AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	
CM.L2-3.4.2			Establish and enforce security configuration settings for information technology products employed in organizational systems.		
3.	Are modifications to technology assets reviewed? [TM:SG4.SP2], [TM:SG4.SP3] <sup>¶</sup>	CM.L2-3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.		
		CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.		
		CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.		
4.	Are integrity requirements used to determine which staff members are authorized to modify information assets? [KIM:SG5.SP1] <sup>¶</sup>	CM.L2-3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.		
5.	Is the integrity of information assets monitored? [KIM:SG5.SP3]	CM.L2-3.4.3	Track, review, approve, or disapprove, and log changes to organizational systems.		

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	6. Are unauthorized or unexplained modifications to technology assets addressed? [TM:SG4.SP2], [TM:SG4.SP3] <sup>¶</sup>	CM.L2-3.4.3 Track, review, approve, or disapprove, and log changes to organizational systems.	
	7. Are modifications to technology assets tested before being committed to production systems? [TM:SG4.SP4] <sup>¶</sup>	CM.L2-3.4.3 Track, review, approve, or disapprove, and log changes to organizational systems. CM.L2-3.4.4 Analyze the security impact of changes prior to implementation.	This practice is intended to be broader than the security impact of a change. Testing should also include functional aspects.
	8. Has a process for managing access to technology assets been implemented? [TM:SG4.SP1]	CM.L2-3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational system.	
	9. Is the maintenance and repair of assets performed and logged in a timely manner? [ADM:SG3.SP2], [TM:SG5.SP2] <sup>¶</sup>	MA.L2-3.7.1 Perform maintenance on organizational systems. MA.L2-3.7.6 Supervise the maintenance activities of personnel without required access authorization.	
	10. Is the maintenance and repair of assets performed with approved and controlled tools and/or methods? [ADM:SG3.SP2], [TM:SG5.SP2] <sup>¶</sup>	MA.L2-3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. MA.L2-3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
	11. Is the remote maintenance and repair of assets approved, logged, and performed in a manner that prevents unauthorized access? [ADM:SG3.SP2], [TM:SG5.SP2] <sup>¶</sup>	MA.L2-3.7.1 Perform maintenance on organizational systems. MA.L2-3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. MA.L2-3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. MA.L2-3.7.6 Supervise the maintenance activities of personnel without required access authorization.	
	<b>Goal 3—Asset configuration baselines are established.</b>		
	1. Do technology assets have configuration baselines? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. CM.L2-3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	2. Is approval obtained for proposed changes to baselines? [TM:SG4.SP3] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	3. Has a baseline of network operations been established? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	4. Is the baseline of network operations managed? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	5. Has a baseline of expected data flows for users and systems been established? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	6. Is the baseline of expected data flows for users and systems managed? [TM:SG4.SP2] <sup>¶</sup>	CM.L2-3.4.1 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
MIL2-Planned	1.	Is there a documented plan for performing change management activities?		
	2.	Is there a documented policy for change management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3.	Have stakeholders for change management activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4.	Have change management standards and guidelines been identified and implemented?		
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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. MA.L2-3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes	
	<b>4 Vulnerability Management</b>				
	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.				
	1.	Has a vulnerability analysis and resolution strategy been developed? [VAR:SG1.SP2]	CA.L2-3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
		People	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
		Information			
		Technology			
		Facilities			
	2.	Is there a standard set of tools and/or methods in use to identify vulnerabilities in assets? [VAR:SG1.SP2]	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
		People			
		Information			
		Technology			
		Facilities			
	3.	Is there a standard set of tools and/or methods in use to detect malicious code in assets? [VAR:SG1.SP2]	AC.L2-3.1.18	Control connection of mobile devices.	
			MA.L2-3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	
			SI.L1-3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	
			SI.L1-3.14.4	Update malicious code protection mechanisms when new releases are available.	
			SI.L1-3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	
	4.	Is there a standard set of tools and/or methods in use to detect unauthorized mobile code in assets? [VAR:SG1.SP2]	AC.L2-3.1.18	Control connection of mobile devices.	
			SC.L2-3.13.13	Control and monitor the use of mobile code.	
			SI.L1-3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	
	5.	Is there a standard set of tools and/or methods in use to monitor assets for unauthorized personnel, connections, devices, and software? [VAR:SG1.SP2]	AC.L2-3.1.12	Monitor and control remote access sessions.	
			AC.L2-3.1.18	Control connection of mobile devices.	
			CM.L2-3.4.9	Control and monitor user-installed software.	
			PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	
			PE.L1-3.10.3	Escort visitors and monitor visitor activity.	
SI.L2-3.14.6			Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.		
SI.L2-3.14.7			Identify unauthorized use of organizational systems.		
SI.L1-3.14.5			Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.		



# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes	
	Goal 2—A process for identifying and analyzing vulnerabilities is established and maintained.				
	1.	Have sources of vulnerability information been identified? [VAR:SG2.SP1] <sup>¶</sup>	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
		Information	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	
		Technology	SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	
		Facilities			
	2.	Is the information from these sources kept current? [VAR:SG2.SP1] <sup>¶</sup>	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
		Information	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	
		Technology	SI.L2-3.14.3	Monitor system security alerts and advisories and take action in response.	
		Facilities			
	3.	Are vulnerabilities being actively discovered? [VAR:SG2.SP2] <sup>¶</sup>	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
		Information	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	
		Technology	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	
		Facilities			
	4.	Are vulnerabilities categorized and prioritized? [VAR:SG2.SP3] <sup>¶</sup>	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	
		Information			
		Technology			
		Facilities			
	5.	Are vulnerabilities analyzed to determine relevance to the organization? [VAR:SG2.SP3] <sup>¶</sup>	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	
		Information	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	
		Technology			
		Facilities			
	6.	Is a repository used for recording information about vulnerabilities and their resolution? [VAR:SG2.SP2] <sup>¶</sup>	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	The listed CUI requirements do not specifically discuss having a repository. A repository directly supports these requirements.
		Information	RA.L2-3.11.3	Remediate vulnerabilities in accordance with risk assessments.	
		Technology	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.	
	Facilities				

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>Goal 3—Exposure to identified vulnerabilities is managed.</b>		
	1. Are actions taken to manage exposure to identified vulnerabilities? [VAR:SG3.SP1] <sup>†</sup>	RA.L2-3.11.3 Remediate vulnerabilities in accordance with risk assessments. CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. SI.L1-3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	
	2. Is the effectiveness of vulnerability mitigation reviewed? [VAR:SG3.SP1] <sup>†</sup>	RA.L2-3.11.3 Remediate vulnerabilities in accordance with risk assessments. CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. SI.L1-3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	
	3. Is the status of unresolved vulnerabilities monitored? [VAR:SG3.SP1] <sup>†</sup>	RA.L2-3.11.3 Remediate vulnerabilities in accordance with risk assessments. CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. SI.L1-3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	
	<b>Goal 4—The root causes of vulnerabilities are addressed.</b>		
	1. Are underlying causes for vulnerabilities identified (through root-cause analysis or other means) and addressed? [VAR:SG4.SP1]	RA.L2-3.11.3 Remediate vulnerabilities in accordance with risk assessments. CA.L2-3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. SI.L1-3.14.1 Identify, report, and correct information and information system flaws in a timely manner.	
MIL-2-Planned	1. Is there a documented plan for performing vulnerability management activities?		
	2. Is there a documented policy for vulnerability management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for vulnerability management activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have vulnerability management standards and guidelines been identified and implemented?		

<sup>†</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes
<b>5 Incident Management</b>				
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.				
1.	Does the organization have a plan for managing incidents? [IMC:SG1.SP1] <sup>¶</sup>	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
2.	Is the incident management plan reviewed and updated? [IMC:SG1.SP1] <sup>¶</sup>	IR.L2-3.6.1 IR.L2-3.6.3	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Test the organizational incident response capability.	
3.	Are the roles and responsibilities in the plan included in job descriptions? [IMC:SG1.SP2]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
4.	Have staff been assigned to the roles and responsibilities detailed in the incident management plan? [IMC:SG1.SP2]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
Goal 2—A process for detecting, reporting, triaging, and analyzing events is established.				
1.	Are events detected and reported (to include cybersecurity events related to personnel activity, network activity, the physical environment, and information)? [IMC:SG2.SP1]	AU.L2-3.3.3 AU.L2-3.3.4 IR.L2-3.6.1 IR.L2-3.6.2 SI.L2-3.14.6 SI.L2-3.14.7 AU.L2-3.3.5	Review and update logged events. Alert in the event of an audit logging process failure. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. Identify unauthorized use of organizational systems. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
2.	Is event data logged in an incident knowledgebase or similar mechanism? [IMC:SG2.SP2]	AU.L2-3.3.3 IR.L2-3.6.1 IR.L2-3.6.2 AU.L2-3.3.5 SI.L2-3.14.3	Review and update logged events. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. Monitor system security alerts and advisories and take action in response.	
3.	Are events categorized? [IMC:SG2.SP4] <sup>¶</sup>	AU.L2-3.3.3 IR.L2-3.6.1 IR.L2-3.6.2 AU.L2-3.3.5	Review and update logged events. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	4. Are events analyzed to determine if they are related to other events? [IMC:SG2.SP4] <sup>†</sup>	AU.L2-3.3.3 Review and update logged events. IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. AU.L2-3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	5. Are events prioritized? [IMC:SG2.SP4] <sup>†</sup>	AU.L2-3.3.3 Review and update logged events. IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. AU.L2-3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	6. Is the status of events tracked? [IMC:SG2.SP4] <sup>†</sup>	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	7. Are events managed to resolution? [IMC:SG2.SP4] <sup>†</sup>	AU.L2-3.3.3 Review and update logged events. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	8. Have requirements (rules, laws, regulations, policies, etc.) for identifying event evidence for forensic purposes been identified? [IMC:SG2.SP3] <sup>†</sup>	AU.L2-3.3.3 Review and update logged events. IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	9. Is there a process to ensure event evidence is handled as required by law or other obligations? [IMC:SG2.SP3] <sup>†</sup>	AU.L2-3.3.3 Review and update logged events. IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	<b>Goal 3—Incidents are declared and analyzed.</b>		
	1. Are incidents declared? [IMC:SG3.SP1]	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	2. Have criteria for the declaration of an incident been established? [IMC:SG3.SP1]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	3. Are incidents analyzed to determine a response? [IMC:SG3.SP2]	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. AU.L2-3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	

<sup>†</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>Goal 4—A process for responding to and recovering from incidents is established.</b>		
	1. Are incidents escalated to stakeholders for input and resolution? [IMC:SG4.SP1]	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	2. Are responses to declared incidents developed and implemented according to pre-defined procedures? [IMC:SG4.SP2]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	3. Are incident status and response communicated to affected parties (including public relations staff and external media outlets)? [IMC:SG4.SP3]	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	4. Are incidents tracked to resolution? [IMC:SG4.SP4]	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	<b>Goal 5—Post-incident lessons learned are translated into improvement strategies.</b>		
	1. Is analysis performed to determine the root causes of incidents? [IMC:SG5.SP1]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	2. Is there a link between the incident management process and other related processes (problem management, risk management, change management, etc.)? [IMC:SG5.SP2]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	3. Are lessons learned from incident management used to improve asset protection and service continuity strategies? [IMC:SG5.SP3]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
MIL2-Planned	1. Is there a documented plan for performing incident management activities?		
	2. Is there a documented policy for incident management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for incident management activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have incident management standards and guidelines been identified and implemented?		

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?	AT.L2-3.2.2     Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes	
	<b>6 Service Continuity Management</b> 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.				
	1.	Are service continuity plans developed and documented for assets required for delivery of the critical service? [SC:SG3.SP2] <sup>¶</sup>	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
		People			
		Information			
		Technology			
		Facilities			
	2.	Are service continuity plans developed using established standards, guidelines, and templates? [SC:SG3.SP2] <sup>¶</sup>	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	3.	Are staff members assigned to execute specific service continuity plans? [SC:SG3.SP3]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	4.	Are key contacts identified in the service continuity plans? [SC:SG2.SP2]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	5.	Are service continuity plans stored in a controlled manner and available to all those who need to know? [SC:SG3.SP4]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	6.	Are availability requirements such as recovery time objectives and recovery point objectives established? [TM:SG5.SP1] <sup>¶</sup>	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	7.	Are mechanisms (e.g., failsafe, load balancing, hot swap capabilities) implemented to achieve resilience requirements in normal and adverse situations? [TM:SG5.SP1]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	Goal 2—Service continuity plans are reviewed to resolve conflicts between plans.				
	1.	Are plans reviewed to identify and resolve conflicts? [SC:SG4.SP2]	IR.L2-3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.



# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>Goal 3 - Service continuity plans are tested to ensure they meet their stated objectives.</b>		
	1. Have standards for testing service continuity plans been implemented? [SC:SG5.SP1] <sup>¶</sup>	IR.L2-3.6.3 Test the organizational incident response capability.	
	2. Has a schedule for testing service continuity plans been established? [SC:SG5.SP1] <sup>¶</sup>	IR.L2-3.6.3 Test the organizational incident response capability.	
	3. Are service continuity plans tested? [SC:SG5.SP3] <sup>¶</sup>	IR.L2-3.6.3 Test the organizational incident response capability.	
	4. Are backup and storage procedures for high-value information assets tested? [KIM:SG6.SP1] <sup>¶</sup>	IR.L2-3.6.3 Test the organizational incident response capability.	
	5. Are test results compared with test objectives to identify needed improvements to service continuity plans? [SC:SG5.SP4]	IR.L2-3.6.3 Test the organizational incident response capability.	
	<b>Goal 4—Service continuity plans are executed and reviewed.</b>		
	1. Have conditions been identified that trigger the execution of the service continuity plan? [SC:SG6.SP1]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	2. <b>Is execution of service continuity plans reviewed?</b> [SC:SG6.SP2] <sup>¶</sup>	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	3. Are improvements identified as a result of executing service continuity plans? [SC:SG7.SP2]	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
MIL2-Planned	1. Is there a documented plan for performing service continuity activities?		
	2. Is there a documented policy for service continuity?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for service continuity activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have service continuity standards and guidelines been identified and implemented?		

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?	AT.L2-3.2.2    Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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	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	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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes	
	<b>7 Risk Management</b>				
	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.				
	1.	Have sources of risk that can affect operations been identified? [RISK:SG1.SP1]	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	2.	Have categories been established for risks? [RISK:SG1.SP1]	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	3.	Has a plan for managing operational risk been established? [RISK:SG1.SP2]	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	4.	Is the plan for managing operational risk communicated to stakeholders? [RISK:SG1.SP2]	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	Goal 2—Risk tolerances are identified, and the focus of risk management activities is established.				
	1.	Have impact areas been identified, such as reputation, financial health, and regulatory compliance? [RISK:SG2.SP2]¶	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	2.	Have impact areas been prioritized to determine their relative importance? [RISK:SG2.SP2]¶	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	3.	Have risk tolerance parameters been established for each impact area? [RISK:SG2.SP2]¶	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	4.	Are risk tolerance thresholds, which trigger action, defined for each category of risk? [RISK:SG2.SP1]	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	Goal 3—Risks are identified.				
	1.	Are operational risks that could affect delivery of the critical service identified? [RISK:SG3.SP2]¶	AT.L2-3.2.1 RA.L2-3.11.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>Goal 4—Risks are analyzed and assigned a disposition.</b>		
	1. Are risks analyzed to determine potential impact to the critical service? [RISK:SG4.SP1] <sup>¶</sup>	RA.L2-3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	2. Is a disposition (accept, transfer, mitigate, etc.) assigned to identified risks? [RISK:SG4.SP3] <sup>¶</sup>	RA.L2-3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	<b>Goal 5—Risks to assets and services are mitigated and controlled.</b>		
	1. Are plans developed for risks that the organization decides to mitigate? [RISK:SG5.SP1]	RA.L2-3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	2. Are identified risks tracked to closure? [RISK:SG5.SP2]	RA.L2-3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
ML2-Planned	1. Is there a documented plan for performing risk management activities?		
	2. Is there a documented policy for risk management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for risk management activities have identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have risk management activities standards and guidelines been identified and implemented?		
ML3-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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?		
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?		

# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes
<b>8 External Dependencies Management</b> 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.				
1.	Are dependencies on external relationships that are critical to the service identified? [EXD:SG1.SP1] <sup>¶</sup>	AC.L1-3.1.1 IA.L1-3.5.1. IA.1-3.5.2. AC.L1-3.1.20	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). Identify system users, processes acting on behalf of users, and devices. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. Verify and control/limit connections to and use of external information systems.	
2.	Has a process been established for creating and maintaining a list of external dependencies? [EXD:SG1.SP1] <sup>¶</sup>	AC.L1-3.1.1 IA.L1-3.5.1. IA.1-3.5.2. AC.L1-3.1.20	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). Identify system users, processes acting on behalf of users, and devices. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. Verify and control/limit connections to and use of external information systems.	
3.	Are external dependencies prioritized? [EXD:SG1.SP2] <sup>¶</sup>	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
Goal 2—Risks due to external dependencies are identified and managed.				
1.	Are risks due to external dependencies identified and managed? [EXD:SG2.SP1] <sup>¶</sup>	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
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] <sup>¶</sup>	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
2.	Are these requirements reviewed and updated? [EXD:SG3.SP2] <sup>¶</sup>	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
3.	Is the ability of external entities to meet resilience requirements of the critical service considered in the selection process? [EXD:SG3.SP3]	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
4.	Are resilience requirements included in formal agreements with external entities? [EXD:SG3.SP4]	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
Goal 4—Performance of external entities is managed.				
1.	Is the performance of external entities monitored against resilience requirements? [EXD:SG4.SP1] <sup>¶</sup>	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	
2.	Has responsibility been assigned for monitoring external entity performance (as related to resilience requirements)? [EXD:SG4.SP1] <sup>¶</sup>	AC.L1-3.1.20	Verify and control/limit connections to and use of external information systems.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	3. Are corrective actions taken as necessary to address issues with external entity performance (as related to resilience requirements)? [EXD:SG4.SP2]	AC.L1-3.1.20 Verify and control/limit connections to and use of external information systems.	
	4. Are corrective actions evaluated to ensure issues are remedied? [EXD:SG4.SP2]	AC.L1-3.1.20 Verify and control/limit connections to and use of external information systems.	
	<b>Goal 5—Dependencies on public services and infrastructure service providers are identified.</b>		
	1. Are public services on which the critical service depends (fire response and rescue services, law enforcement, etc.) identified? [EC:SG4.SP3]	AC.L1-3.1.20 Verify and control/limit connections to and use of external information systems.	
	2. Are infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) identified? [EC:SG4.SP4]	AC.L1-3.1.20 Verify and control/limit connections to and use of external information systems.	
ML2-Planned	1. Is there a documented plan for performing external dependency management activities?		
	2. Is there a documented policy for external dependency management?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for external dependency management activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have external dependency management activities standards and guidelines been identified and implemented?		
ML3-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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	3. Is there adequate funding to perform external dependency management activities as planned?		
	4. Are risks related to the performance of planned external dependency management activities identified, analyzed, disposed of, monitored, and controlled?		
ML4-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?		

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?		



# CYBER RESILIENCE ANALYSIS

Cyber Resilience Analysis		CMMC Practice and Description		Notes
<b>9 Training and Awareness</b>				
The purpose of Training and Awareness is to develop skills and promote awareness for people with roles that support the critical service.				
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] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
2.	Have required cyber security skills been identified for specific roles (administrators, technicians, etc.) for the critical service? [HRM:SG1.SP1]	AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
3.	Are skill gaps present in personnel responsible for cyber security identified? [OTA:SG3.SP1] <sup>¶</sup>	AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
4.	Have cyber security training needs been identified? [OTA:SG3.SP1] <sup>¶</sup>	AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
Goal 2—Awareness and training activities are conducted.				
1.	Are cyber security awareness activities for the critical service conducted? [OTA:SG2.SP1] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
2.	Are cyber security training activities for the critical service conducted? [OTA:SG4.SP1] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
3.	Is the effectiveness of the awareness and training programs evaluated? [OTA:SG2.SP3, OTA:SG4.SP3]	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
		AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
4.	Are awareness and training activities revised as needed? [OTA:SG1.SP3], [OTA:SG3.SP3]	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
		AT.L2-3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
5.	Have privileged users been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
6.	Have senior executives been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
7.	Have physical and information security personnel been trained in their specific roles and responsibilities in support of the critical service? [OTA:SG4.SP1] <sup>¶</sup>	AT.L2-3.2.1	Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
		AT.L2-3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
MIL2-Planned	1.	Is there a documented plan for performing training activities?		
	2.	Is there a documented policy for training?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3.	Have stakeholders for training activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4.	Have training standards and guidelines been identified and implemented?		
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?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis	CMMC Practice and Description	Notes
	<b>10 Situational Awareness</b> 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.		
	<b>Goal 1—Threat monitoring is performed.</b>		
	1. Has responsibility for monitoring sources of threat information been assigned? [MON:SG1.SP2]	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	2. Have threat monitoring procedures been implemented? [MON:SG2.SP2] <sup>¶</sup>	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	3. Have resources been assigned and trained to perform threat monitoring? [MON:SG2.SP3] <sup>¶</sup>	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	<b>Goal 2—The requirements for communicating threat information are established.</b>		
	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]	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	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]	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	<b>Goal 3—Threat information is communicated.</b>		
	1. Is threat information communicated to stakeholders? [COMM:SG3.SP2]	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	2. Have resources been assigned authority and accountability for communicating threat information? [COMM:SG2.SP3]	SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
	3. Have resources been trained with respect to their specific role in communicating threat information? [COMM:SG2.SP3]	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. SI.L2-3.14.3 Monitor system security alerts and advisories and take action in response.	
MIL2-Planned	1. Is there a documented plan for performing situational awareness activities?		
	2. Is there a documented policy for situational awareness?	AT.L2-3.2.1 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	3. Have stakeholders for situational awareness activities been identified and made aware of their roles?	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	4. Have situational awareness standards and guidelines been identified and implemented?		

<sup>¶</sup> Denotes a Cyber Hygiene practice.

# CYBER RESILIENCE ANALYSIS

	Cyber Resilience Analysis		CMMC Practice and Description	Notes
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?	AT.L2-3.2.2    Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	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?		
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?		
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?		

# CYBER RESILIENCE ANALYSIS

## Crosswalk Reference Key

Cyber Resilience Analysis (CRA) Reference Key	
<b>AM</b>	Asset Management
<b>CCM</b>	Configuration and Change Management
<b>CM</b>	Controls Management
<b>EDM</b>	External Dependencies Management
<b>IM</b>	Incident Management
<b>RM</b>	Risk Management
<b>SA</b>	Situational Awareness
<b>SCM</b>	Service Continuity Management
<b>TA</b>	Training and Awareness
<b>VM</b>	Vulnerability Management
<b>Gx</b>	Goal
<b>Qx</b>	Question
<b>P</b>	People
<b>I</b>	Information
<b>T</b>	Technology
<b>F</b>	Facilities
<b>MIL</b>	CRA Maturity Indicator Level

<b>RMM</b>	<a href="https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084">https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084</a>
<b>CMMC</b>	<a href="https://www.acq.osd.mil/cmmc/">https://www.acq.osd.mil/cmmc/</a>

CERT® Resilience Management Model (CERT® RMM) Reference Key*	
<b>ADM</b>	Asset Definition and Management
<b>AM</b>	Access Management
<b>COMM</b>	Communications
<b>COMP</b>	Compliance
<b>CTRL</b>	Controls Management
<b>EC</b>	Environmental Control
<b>EF</b>	Enterprise Focus
<b>EXD</b>	External Dependencies Management
<b>HRM</b>	Human Resource Management
<b>IMC</b>	Incident Management and Control
<b>KIM</b>	Knowledge and Information Management
<b>MON</b>	Monitoring
<b>OTA</b>	Organizational Training and Awareness
<b>RISK</b>	Risk Management
<b>RRD</b>	Resilience Requirements Development
<b>RTSE</b>	Resilience Technical Solution Engineering
<b>SC</b>	Service Continuity
<b>TM</b>	Technology Management
<b>VAR</b>	Vulnerability Awareness and Resolution
<b>SGx</b>	Specific Goal
<b>SPx</b>	Specific Practice
<b>GGx</b>	Generic Goal
<b>GPx</b>	Generic Practice

\* RMM references for the CRA questions can be found in the CRA to CMMC Crosswalk starting on page 12.

CYBER RESILIENCE  
**ANALYSIS**

This page is intentionally blank.

