www.SP6.io

Cyber Risk Basics for IT Professionals

Day-to-Day Cyber Risk Management

Visit Ascera.com for the Extended Version

Managing Risks

Threats and Vulnerabilities

Adversarial

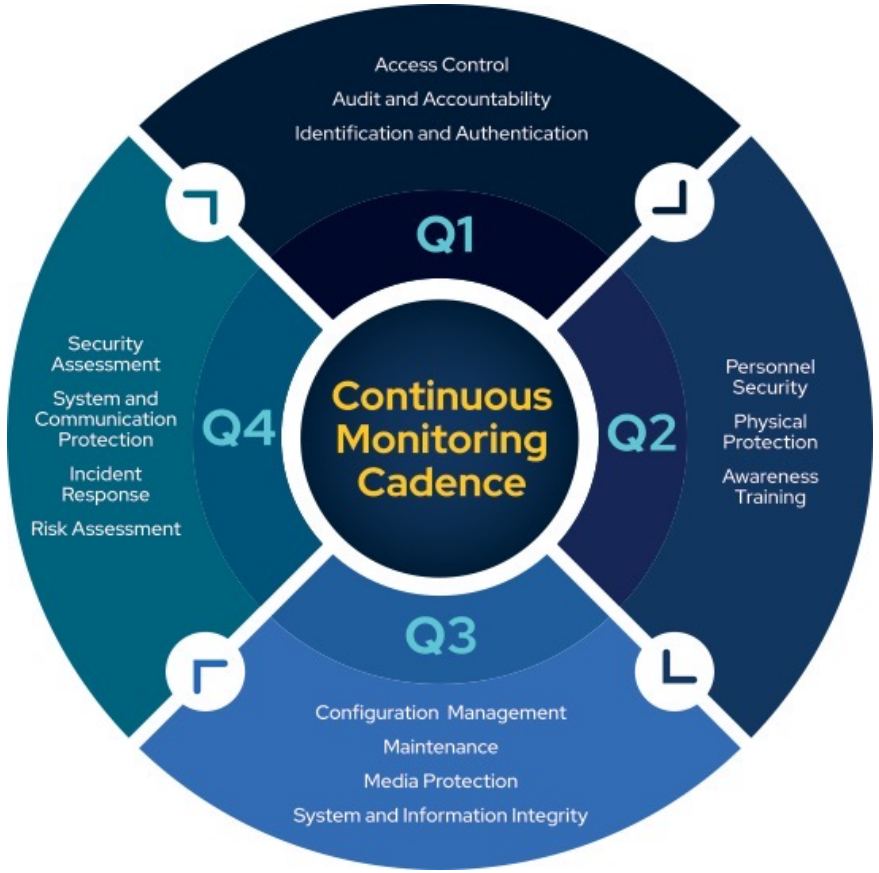
1. Outsider
2. Approved Insider
3. Insider
4. Privileged Insider

Non-Adversarial

1. Accidental Use/ Access Display/ Release
2. Fire
3. Flood
4. Storm/Tornado

Security Controls

CMMC/NIST 800-171



Potential Impact

Federal Govt

1. National Security
2. DoD Objectives
3. Economic Freedom

DIB/Private Sector

1. Financial Loss
2. Damaged Reputation
3. Image
4. Business/Mission Objectives
5. Privacy
6. Safety
7. Competitive Advantag
8. Intellectual Property

Managing Risks

Threats and Vulnerabilities

(Granular)

Adversarial

1. Unauthorized Access
2. Ransomware
3. Malware
4. Privilege escalation
5. Man-in-the-middle
6. DDoS
7. Phishing

Non-Adversarial

1. Accidental User Access
2. Fire
3. Flood
4. Storm/Tornado
5. Incorrect system configuration
6. Unintended display or release

Potential

Security Controls

CMMC/NIST 800-171

Personnel Security	Security Assessment
Physical Protection	System and Communication Protection
Awareness & Training	Incident Response
Configuration Management	Risk Assessment
Maintenance	Access Control
Media Protection	Audit and Accountability
System and Information Integrity	Identification and Authentication

Reduced

Potential Impact

Federal Govt

1. National Security
2. DoD Objectives
3. Economic Freedom

DIB/Private Sector

1. Financial Loss
2. Damaged Reputation
3. Image
4. Business/Mission Objectives
5. Privacy
6. Safety
7. Competitive Advantag
8. Intellectual Property

Conducting a Risk Assessment of a CMMC Program

Start the Assessment

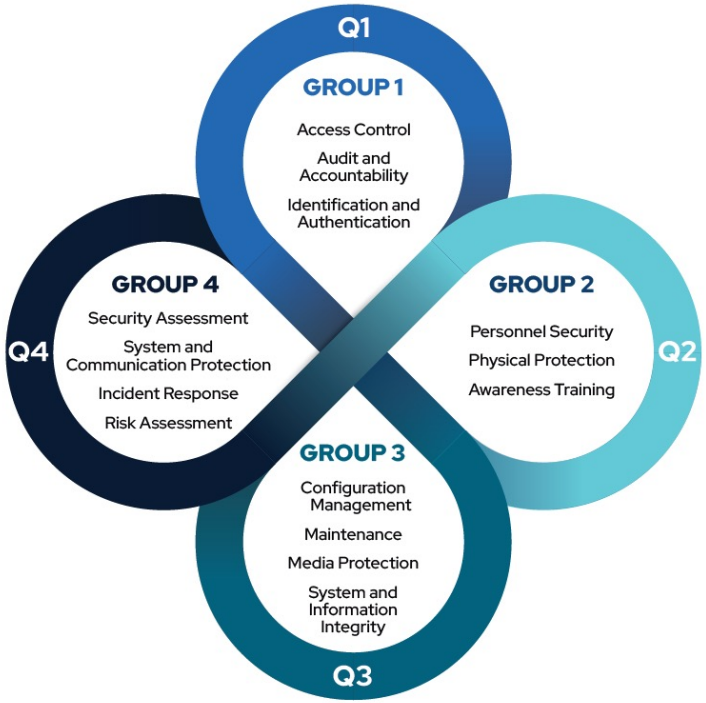
Prepare for the Risk Assessment

1. **Document the Purpose:**
   - Initial, comparative, other
   - To inform a major decision
2. **Identify the Scope**
   - Enterprise/Business Level
   - System or Control level
3. **Document Assumptions & Constraints**
   - About the threats and vulnerabilities
   - About resources
4. **Identify sources of threats, vulnerability and impact**
   - See previous slide
5. **Identify the risk model and analytic approach**

Perform the Assessment

CMMC/NIST 800-171

Assessment Activity Cadence



Using NIST 800-171A, assess each control at the assessment objective level and use the DoDAM Weighted criteria of 5, 3, 1

Report the Results

Risk Assessment Report

1. **Valid Dates for the Risk Assessment**
2. **Summary of the Purpose and Scope**
3. **State whether this is an initial or subsequent RA**
4. **Describe the Overall Risk**
5. **List the Identified Risks**
6. **Summarize the Purpose of RA and the assumptions**

ConMon

Monitor the risk factors by conducting ongoing monitoring of operations, assets, individuals, suppliers, or the DoD. Update as needed

Conducting a Risk Assessment of a CMMC Program

Perform the Assessment

CMMC/NIST 800-171

Security Family	Identifier	Security Requirement	Assessment Objective	Status	Likelihood	Confidentiality	Integrity	Availability	Impact Aggregate (in Alignment with DoDAM)	Risk Rating	Risk Treatment Option
Access Control	3.1.3	**Control the flow of CUI in accordance with approved authorizations.**	Determine if:								
Access Control	3.1.3(a)		Information flow control policies are defined.	0-Met	1	3			1	Low	Accept
Access Control	3.1.3(b)		Methods and enforcement mechanisms for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(c)		Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.	0-Met							
Access Control	3.1.3(d)		Authorizations for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(e)		Approved authorizations for controlling the flow of CUI are enforced.	0-Met							

Conducting a Risk Assessment of a CMMC Program

SP6

Perform the Assessment

CMMC/NIST 800-171

Cyber Risk Basics

Risk Model – NIST 800-171A and NIST 800-30

Security Family	Identifier	Security Requirement	Assessment Objective	Status	Likelihood	Confidentiality	Integrity	Availability	Impact Aggregate (in Alignment with DoDAM)	Risk Rating	Risk Treatment Option
Access Control	3.1.3	**Control the flow of CUI in accordance with approved authorizations.**	Determine if:								
Access Control	3.1.3(a)		Information flow control policies are defined.	0-Met							
Access Control	3.1.3(b)		Methods and enforcement mechanisms for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(c)		Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.	0-Met	1	3			1	Low	Accept
Access Control	3.1.3(d)		Authorizations for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(e)		Approved authorizations for controlling the flow of CUI are enforced.	0-Met							

Control Family, Control, and Control Objectives

Conducting a Risk Assessment of a CMMC Program

SP6

Perform the Assessment

CMMC/NIST 800-171

Cyber Risk Basics

Risk Model – NIST 800-171A and NIST 800-30

Security Family	Identifier	Security Requirement	Assessment Objective	Status	Likelihood	Confidentiality	Integrity	Availability	Impact Aggregate (in Alignment with DoDAM)	Risk Rating	Risk Treatment Option
Access Control	3.1.3	**Control the flow of CUI in accordance with approved authorizations.**	Determine if:								
Access Control	3.1.3(a)		Information flow control policies are defined.	0-Met	1	3			1	Low	Accept
Access Control	3.1.3(b)		Methods and enforcement mechanisms for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(c)		Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.	0-Met							
Access Control	3.1.3(d)		Authorizations for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(e)		Approved authorizations for controlling the flow of CUI are enforced.	0-Met							

Risk = Likelihood x Impact

Conducting a Risk Assessment of a CMMC Program

SP6

Perform the Assessment

CMMC/NIST 800-171

Cyber Risk Basics

Risk Model – NIST 800-171A and NIST 800-30

Security Family	Identifier	Security Requirement	Assessment Objective	Status	Likelihood	Confidentiality	Integrity	Availability	Impact Aggregate (in Alignment with DoDAM)	Risk Rating	Risk Treatment Option
Access Control	3.1.3	**Control the flow of CUI in accordance with approved authorizations.**	Determine if:								
Access Control	3.1.3(a)		Information flow control policies are defined.	0-Met							
Access Control	3.1.3(b)		Methods and enforcement mechanisms for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(c)		Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.	0-Met	1	3			1	Low	Accept
Access Control	3.1.3(d)		Authorizations for controlling the flow of CUI are defined.	0-Met							
Access Control	3.1.3(e)		Approved authorizations for controlling the flow of CUI are enforced.	0-Met							

Risk = Likelihood x Impact

Likelihood this will become a compliance risk? Or will a threat be realized?

Confidentiality of CUI is at least Moderate per the DoD / USG

Based on the DoD Assessment Methodology

Risk Assessment

Cyber Risk Basics for IT Professionals

Qualitative Values	Semi-Quantitative		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned, or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not fully implemented; control(s) are partially implemented and at least minimally effective
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective

Manage Your Risks – Daily