Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:
Building a CMMC Model: 3.1.11 Risk Assessment Policy, Security Assessment Reports

January 24| 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

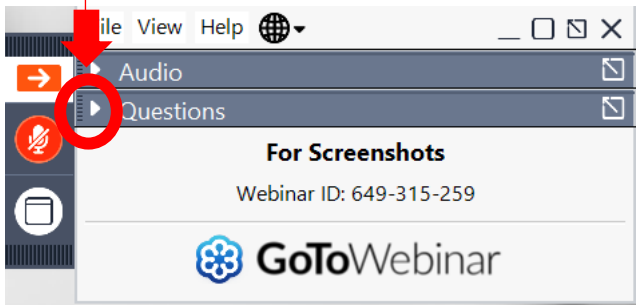
PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

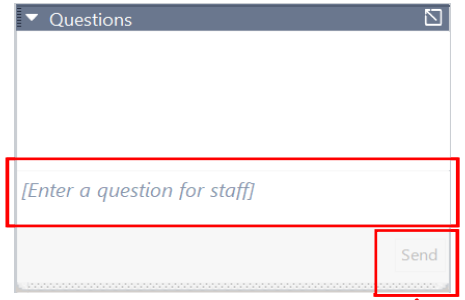
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

Wisconsin Procurement Institute

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

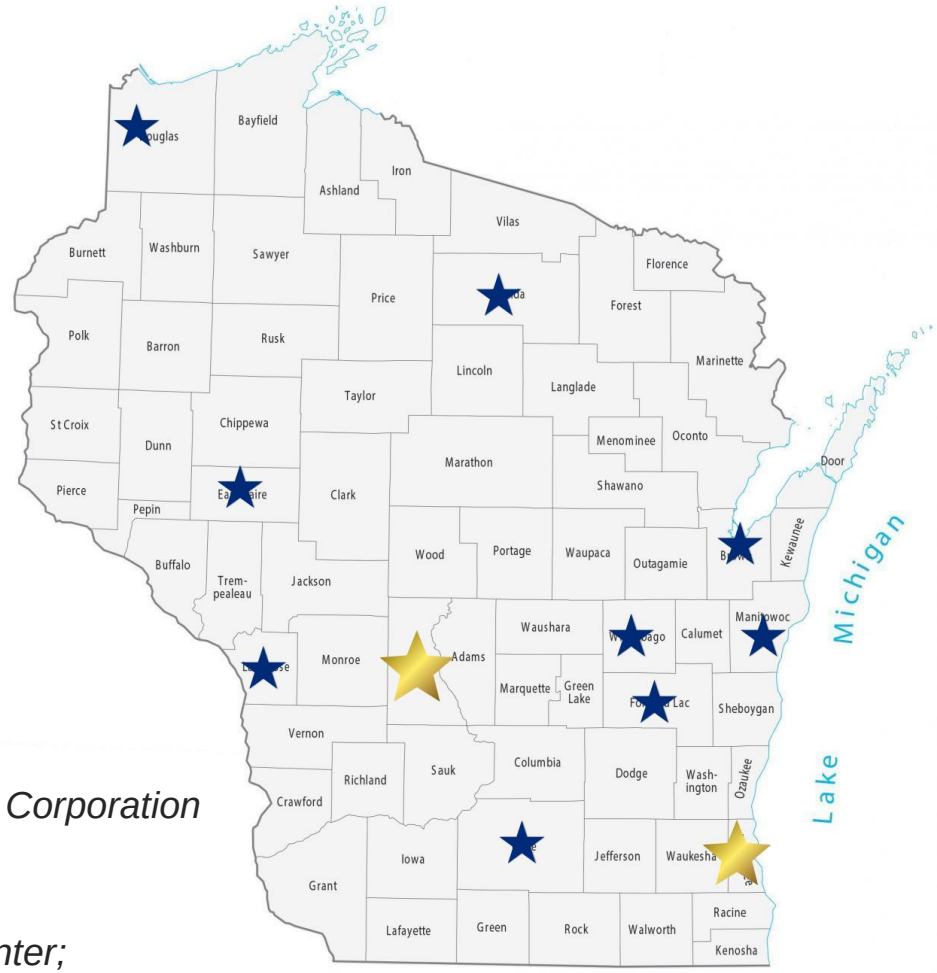
WPI provides services to all of Wisconsin's 72 counties

- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

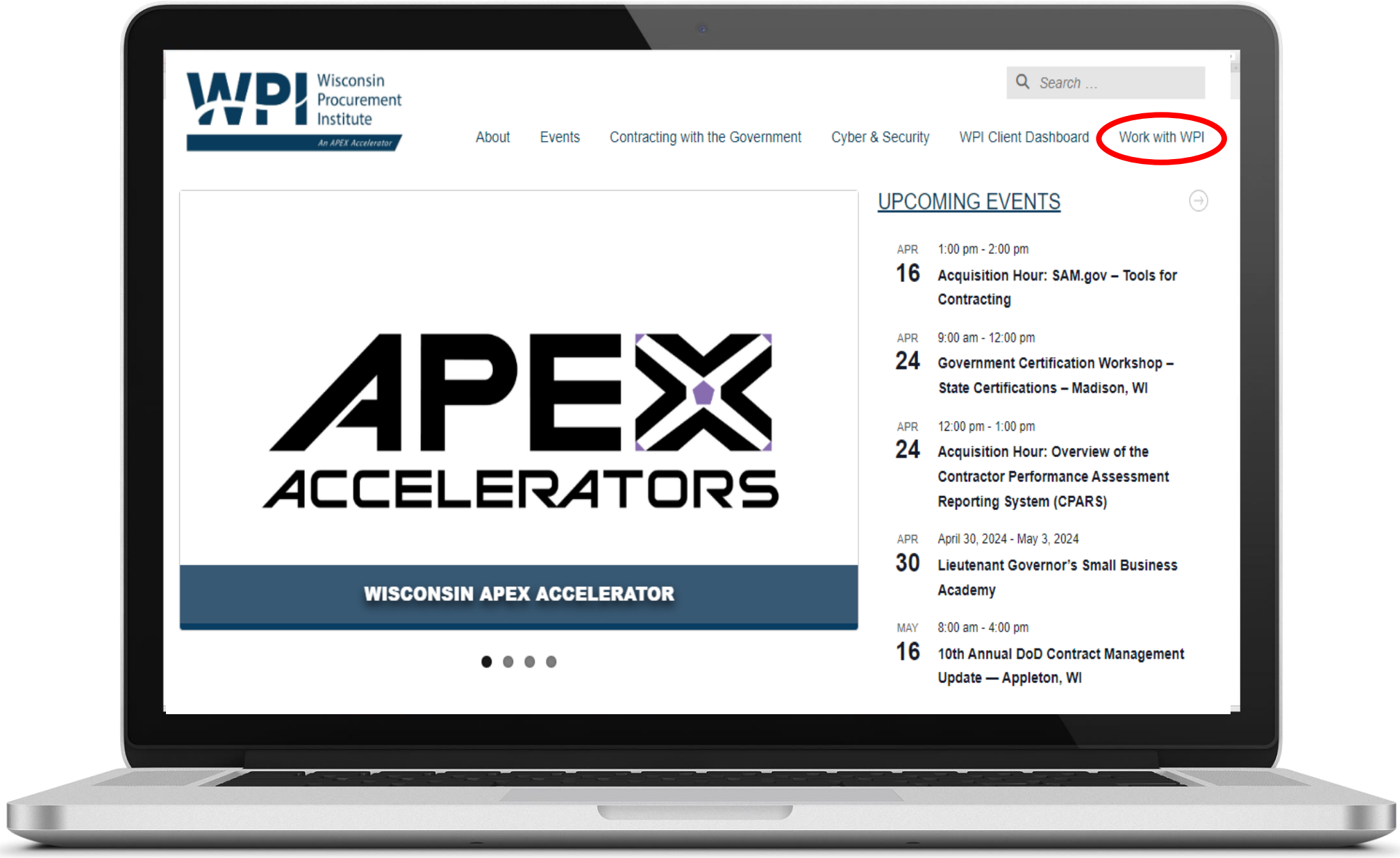
www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



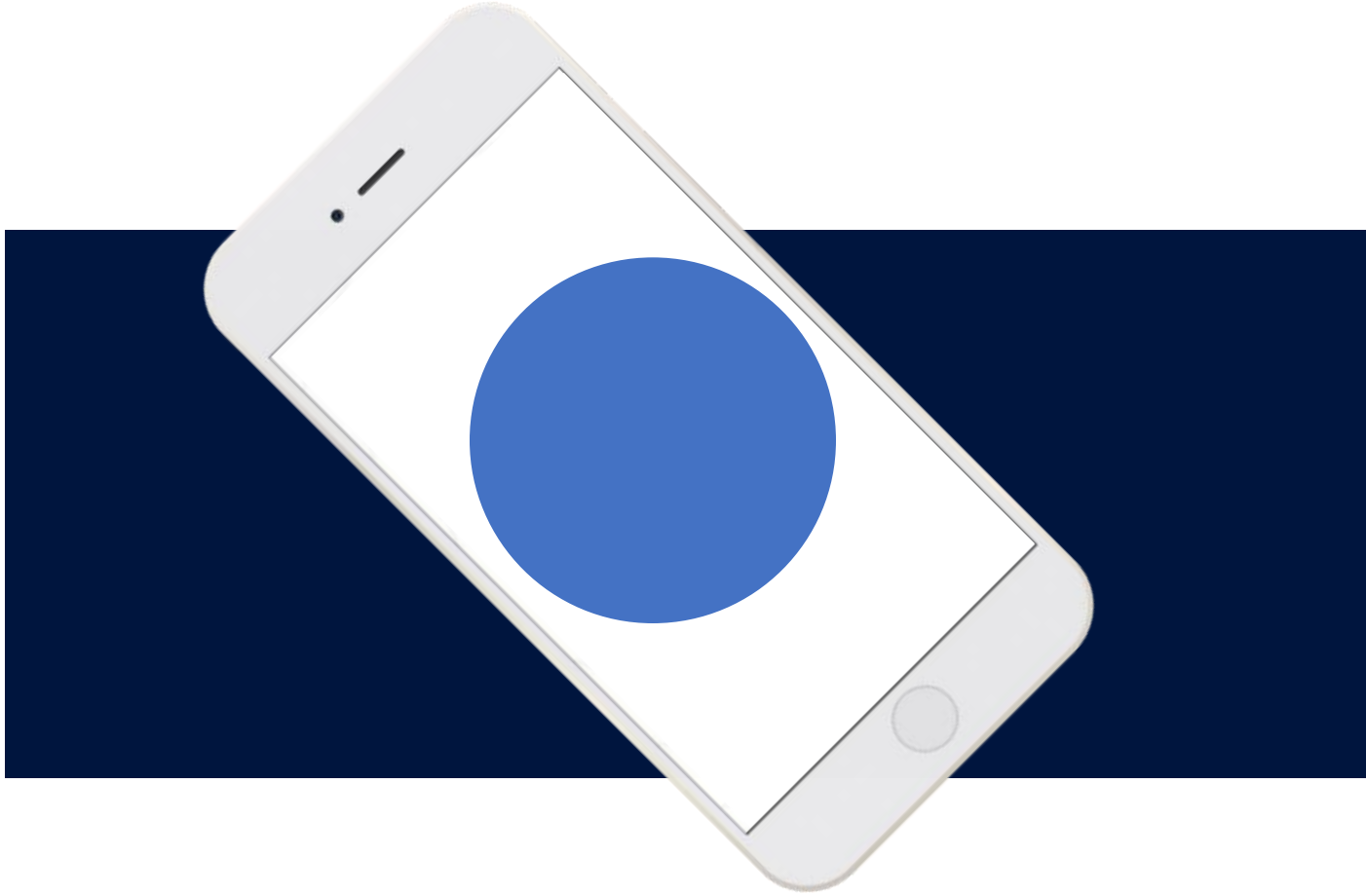
Wisconsin Procurement Institute
An APEX Accelerator


WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Documentation for NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

An APEX Accelerator



CYBER FRIDAY SESSIONS – January 24th, 2025

DFARS 252.204-7012

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

The Contractor shall notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement.

When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract… the Contractor shall rapidly report cyber incidents to DoD.

DFARS 252.204-7021

The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices…

(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

14 Families – 110 Controls – 320 Audit Objectives

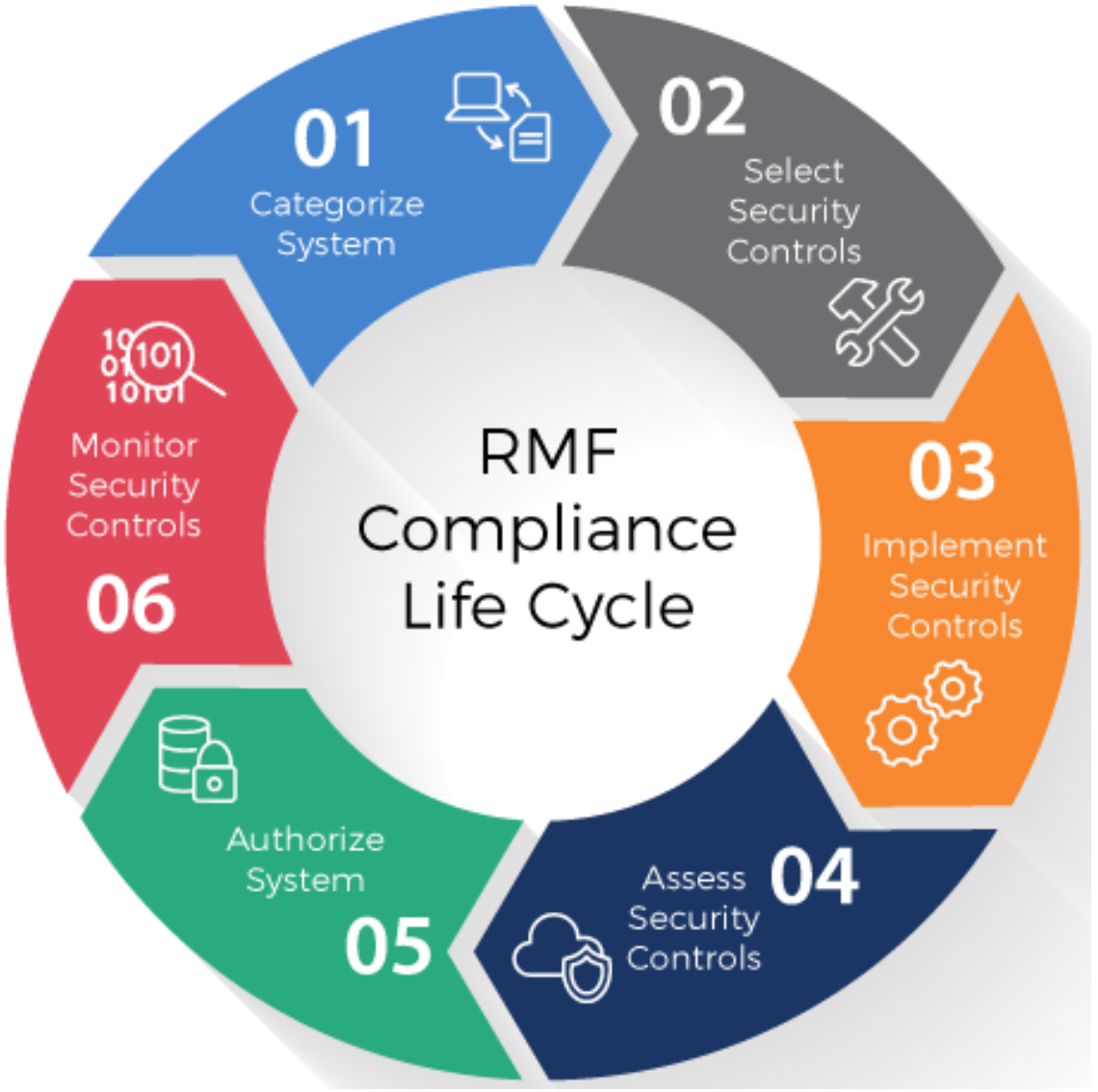
- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- **Risk Assessment**
- **Security Assessment**
- System and Communications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

NIST Handbook 162

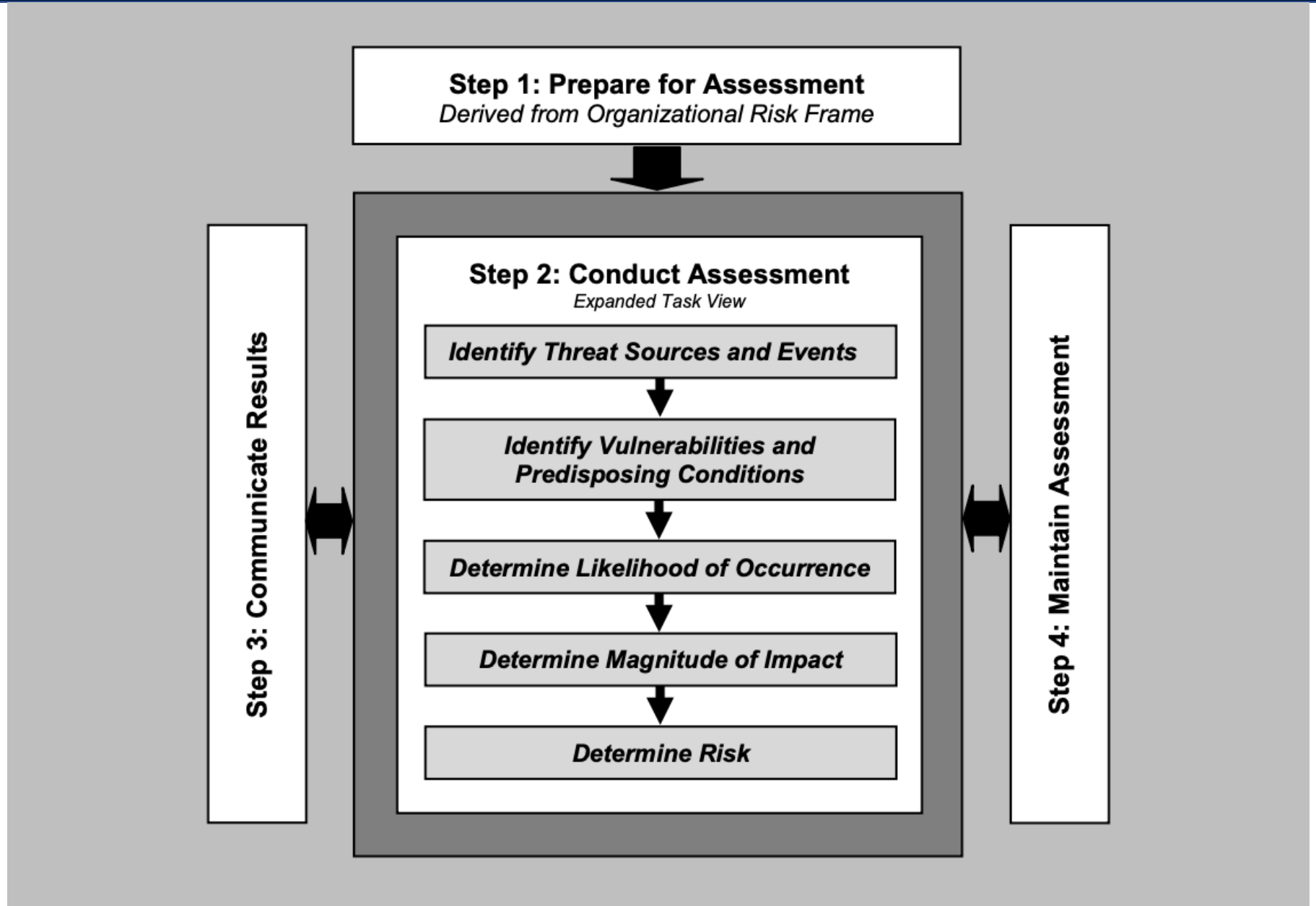
NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

1. NIST SP 800-30 r1 — Guide for Conducting Risk Assessments
2. NIST SP 800-171A — NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information
3. NIST SP 800-115 — Technical Guide to Information Security Testing and Assessment

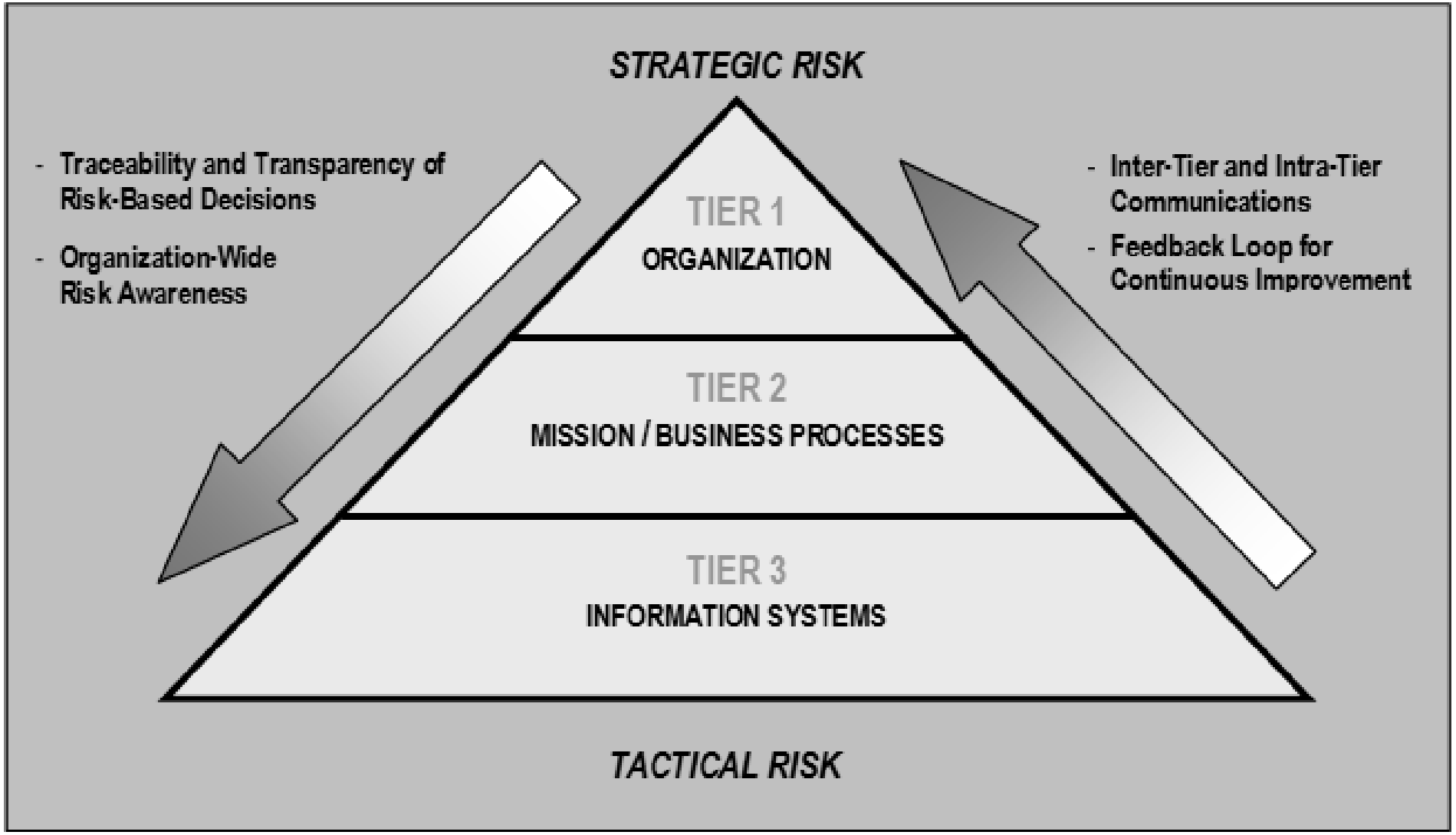
NIST Risk Management Framework



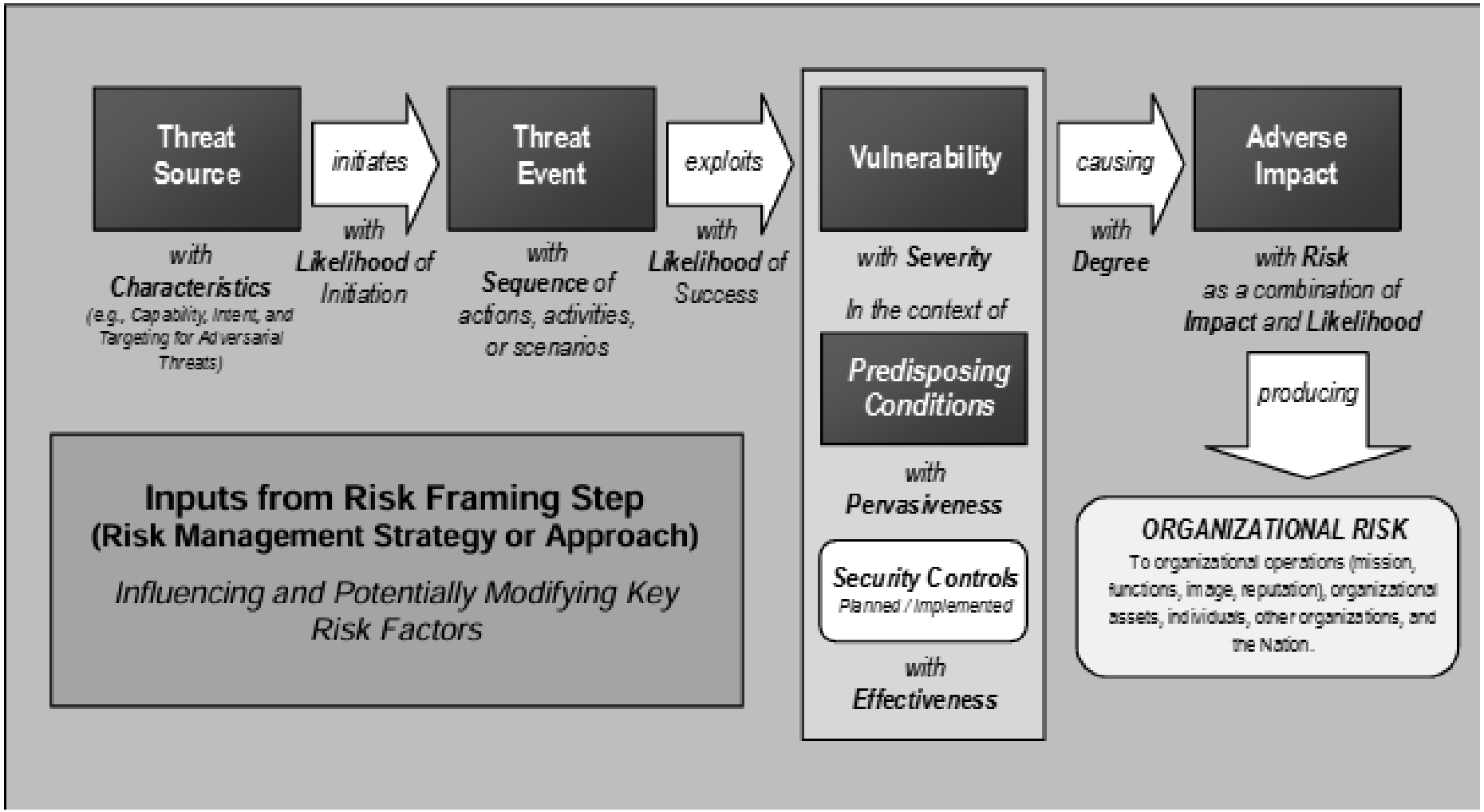
Risk Assessment Process



Risk Assessments

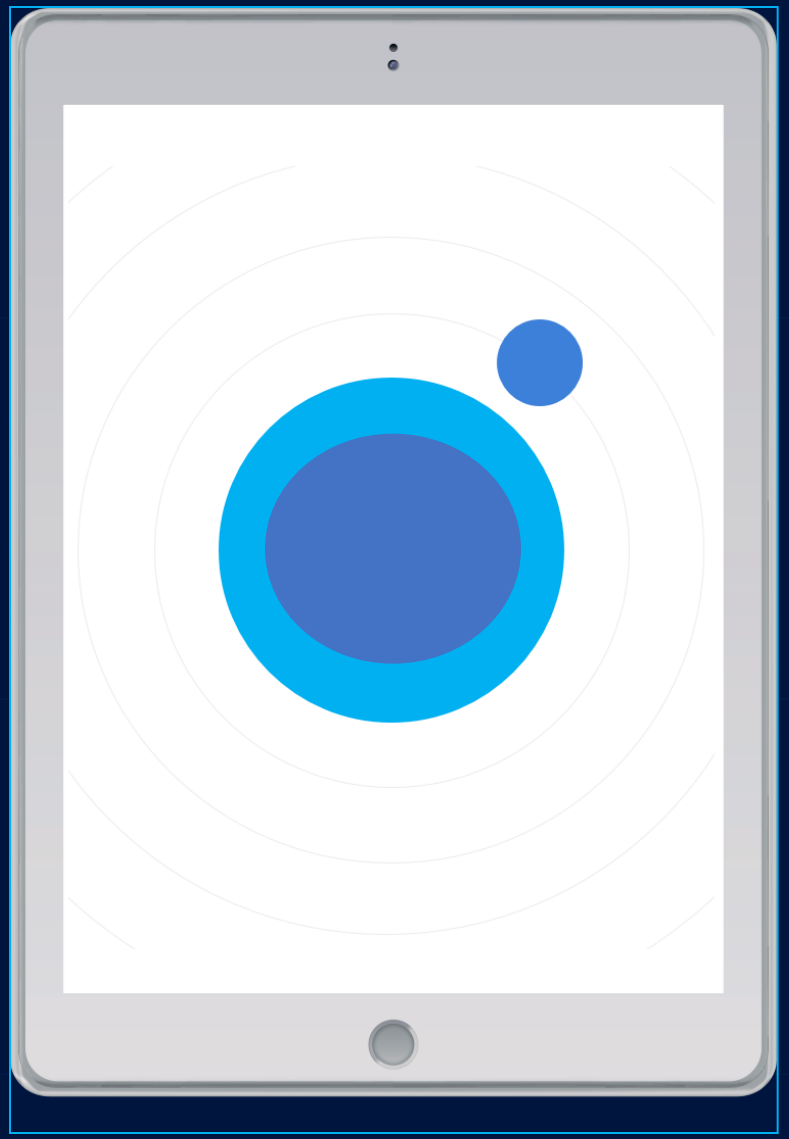


Assessing Risk



3.11.1	**SECURITY REQUIREMENT** 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.
	ASSESSMENT OBJECTIVE *Determine if:* **3.11.1[a]** *the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.* **3.11.1[b]** *risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].

Risk Assessment Policy



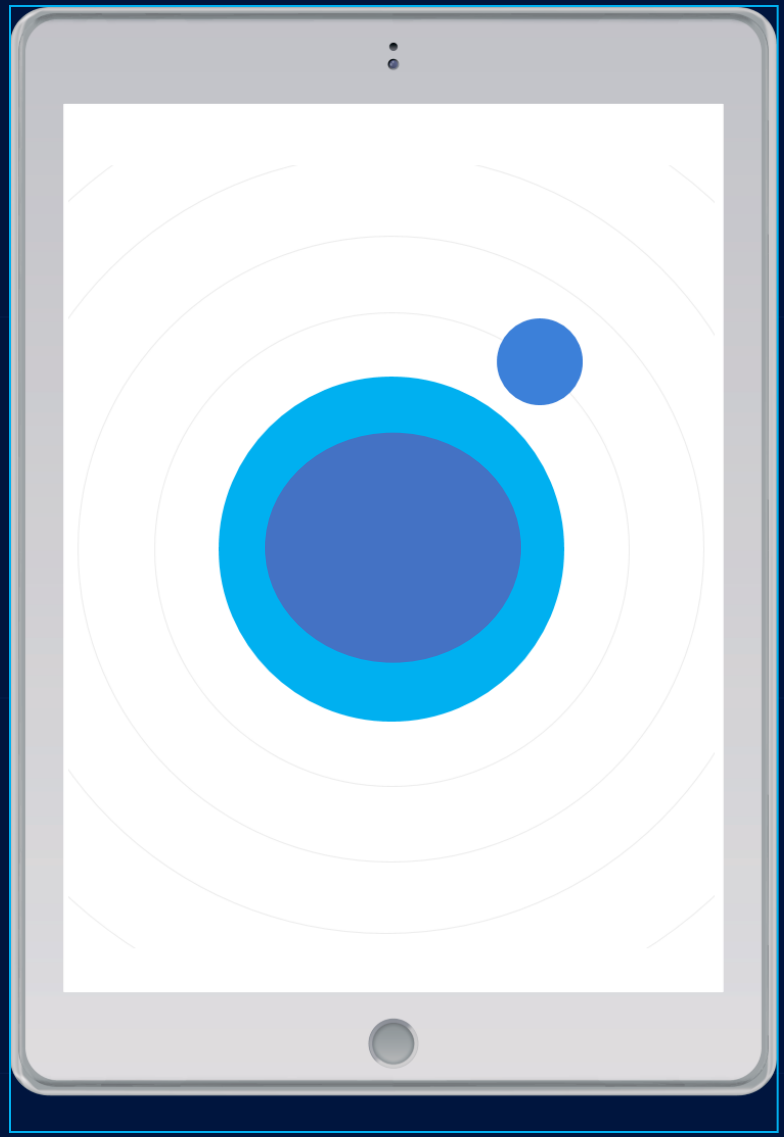
1. Purpose
2. Scope
3. Policy Statement
4. Process
    1. Assumptions and Constraints
    2. Sources of Information on Threats, Vulnerabilities, and Potential Impact
    3. Risk Model and Approach

3. Policy Statements

3.1 Risk Assessment Procedures

- **Identify Threat Sources**
- **Identify Threat Events**
- **Identify Vulnerabilities within the Organization**
- **Determine the Likelihood of Successful Events**
- **Determine the Adverse Impacts of Successful Events**
- **Determine Information Security Risks as a combination of likelihood and impact.**

Elements of the Policy



3.11.2	SECURITY REQUIREMENT Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.2[a]	*the frequency to scan for vulnerabilities in organizational systems and applications is defined.*
	3.11.2[b]	*vulnerability scans are performed on organizational systems with the defined frequency.*
	3.11.2[c]	*vulnerability scans are performed on applications with the defined frequency.*
	3.11.2[d]	*vulnerability scans are performed on organizational systems when new vulnerabilities are identified.*
	3.11.2[e]	*vulnerability scans are performed on applications when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].	

3.11.3	**SECURITY REQUIREMENT** Remediate vulnerabilities in accordance with risk assessments.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.11.3[a] *vulnerabilities are identified.*
	3.11.3[b] *vulnerabilities are remediated in accordance with risk assessments.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis responsibilities; personnel with vulnerability remediation responsibilities; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting or implementing vulnerability scanning, analysis, remediation, and information sharing].

NIST Special Publication 800-30
Revision 1

Guide for Conducting Risk Assessments

National Institute of Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

Appendices D, E, F, G, H, I, J, K

Risk Assessment Summary Report

System Name: [Insert System Name]
Assessment Date: [Insert Date]
Assessed By: [Insert Assessor Name]
System Owner: [Insert Owner Name]

---

1. Executive Summary

Overall Risk Level: [Low / Moderate / High]
Key Findings:

- [Summarized risk finding 1]
- [Summarized risk finding 2]
- [Summarized risk finding 3]

Top Risks:

1. [High-risk issue 1]
2. [High-risk issue 2]
3. [High-risk issue 3]

Recommended Actions:

- [Action 1]
- [Action 2]
- [Action 3]

---

2. Identified Risks

Risk ID	Threat	Vulnerability	Impact	Likelihood	Risk Level
1	[Threat 1]	[Vulnerability 1]	High	High	High
2	[Threat 2]	[Vulnerability 2]	Medium	High	Medium
3	[Threat 3]	[Vulnerability 3]	Low	Medium	Low

3. Risk Prioritization

Critical Risks:

1. [Critical Risk 1] – [Impact]
2. [Critical Risk 2] – [Impact]
3. [Critical Risk 3] – [Impact]

---

4. Recommended Mitigation Actions

Risk ID	Recommended Action	Owner	Due Date	Status
1	[Mitigation 1]	[Owner]	[Date]	[Open/Closed]
2	[Mitigation 2]	[Owner]	[Date]	[Open/Closed]
3	[Mitigation 3]	[Owner]	[Date]	[Open/Closed]

---

5. Conclusion

Overall System Risk: [Acceptable / Requires Immediate Action / Ongoing Monitoring]

Next Steps:

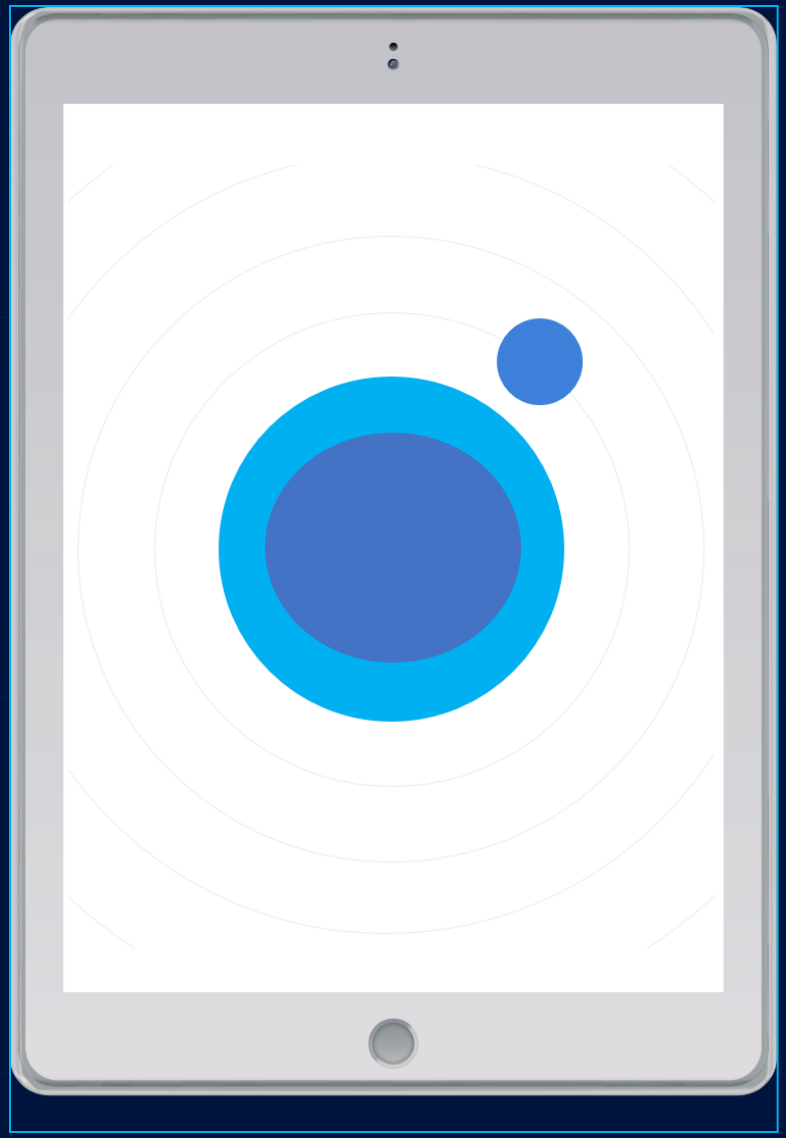
- [Step 1]
- [Step 2]
- [Step 3]

---

6. Appendices

- Vulnerability Scan Results
- Supporting Evidence
- Detailed Risk Analysis

Security Assessment Policy



1. Purpose
2. Scope
3. Policy Statement
4. Process
    1. Planning
    2. Execution
    3. Post-Execution

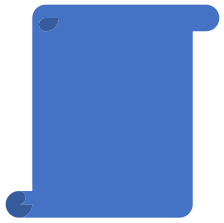
Security Assessment Methods

NIST Special Publication 800-171A

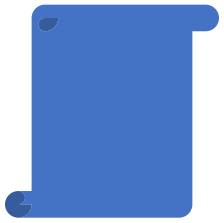
Assessing Security Requirements for Controlled Unclassified Information

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.12.1[a] *the frequency of security control assessments is defined.*
	3.12.1[b] *security controls are assessed with the defined frequency to determine if the controls are effective in their application.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with security assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].

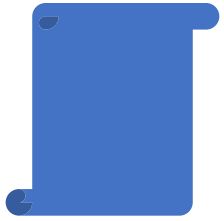
Important Notes about Security Assessments



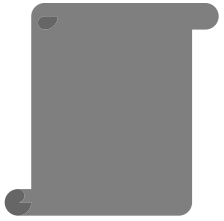
All Controls must be assessed at least annually.



All Controls must be identified and defined in System Security Plan



Assessment Methodology must be declared and followed.



NIST SP 800-171A provides assessment framework

Important Note

Organizations are not expected to employ *all* assessment methods and objects contained within the assessment procedures identified in this publication. Rather, organizations have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the organization can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination that the CUI requirements have been satisfied.

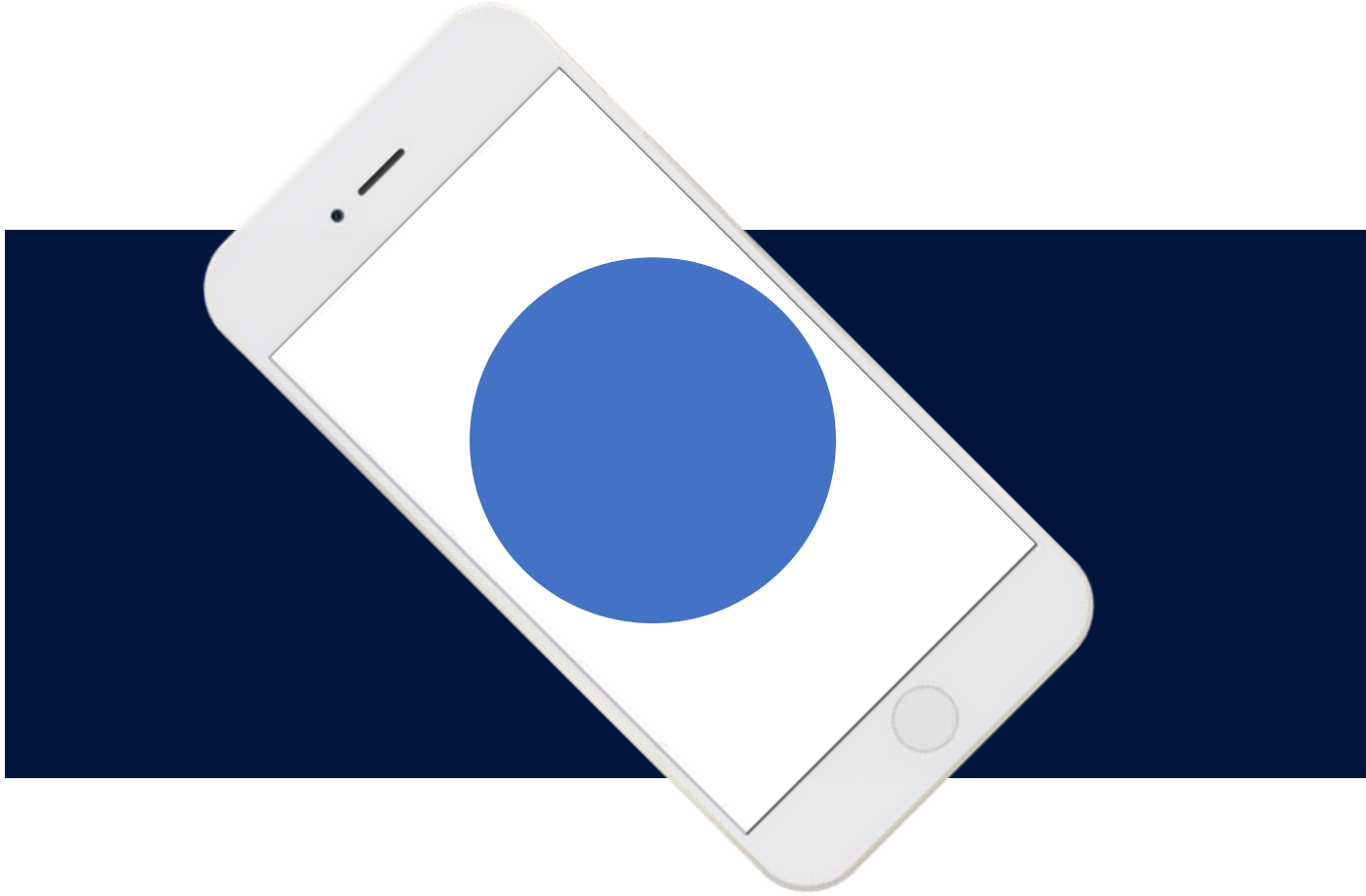
3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.12.2[a] *deficiencies and vulnerabilities to be addressed by the plan of action are identified.*
	3.12.2[b] *a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	3.12.2[c] *the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms for developing, implementing, and maintaining plan of action].

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

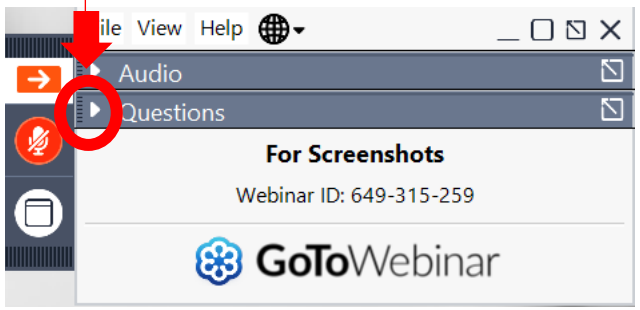
An APEX Accelerator



QUESTIONS?

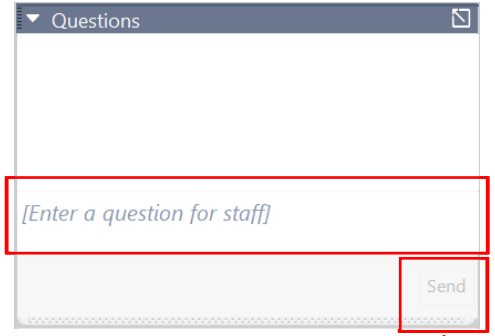
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

CYBER FRIDAY LIVE WEBINAR SERIES

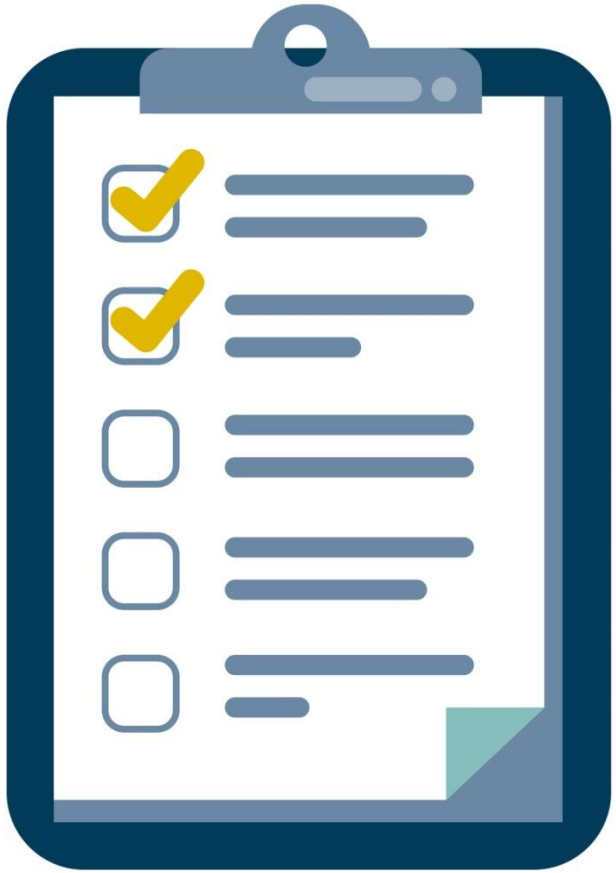
Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **February 28** – CMMC: Are You Ready for a C3PAO Assessment?
- **March 28** – CMMC: Federal Cybersecurity Requirements – Who Must Comply?
- **April 25** – CMMC: Maintaining Your CMMC Certification

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

January 24, 2025

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Neelu Patil
neelagangap@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226