Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Model: 3.1.6 Incident Response Policy, Incident Response Plan

September 20 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

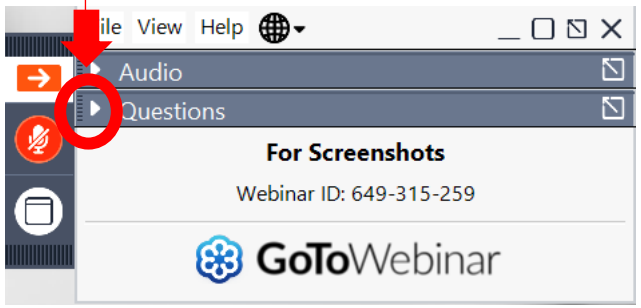
PLEASE

- 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!

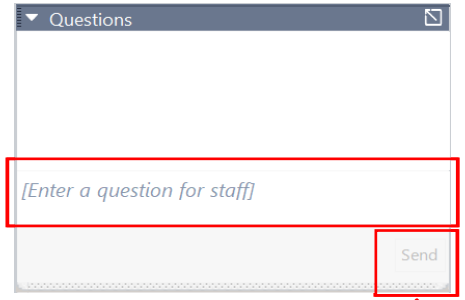
OPENING THE QUESTIONS BOX

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.

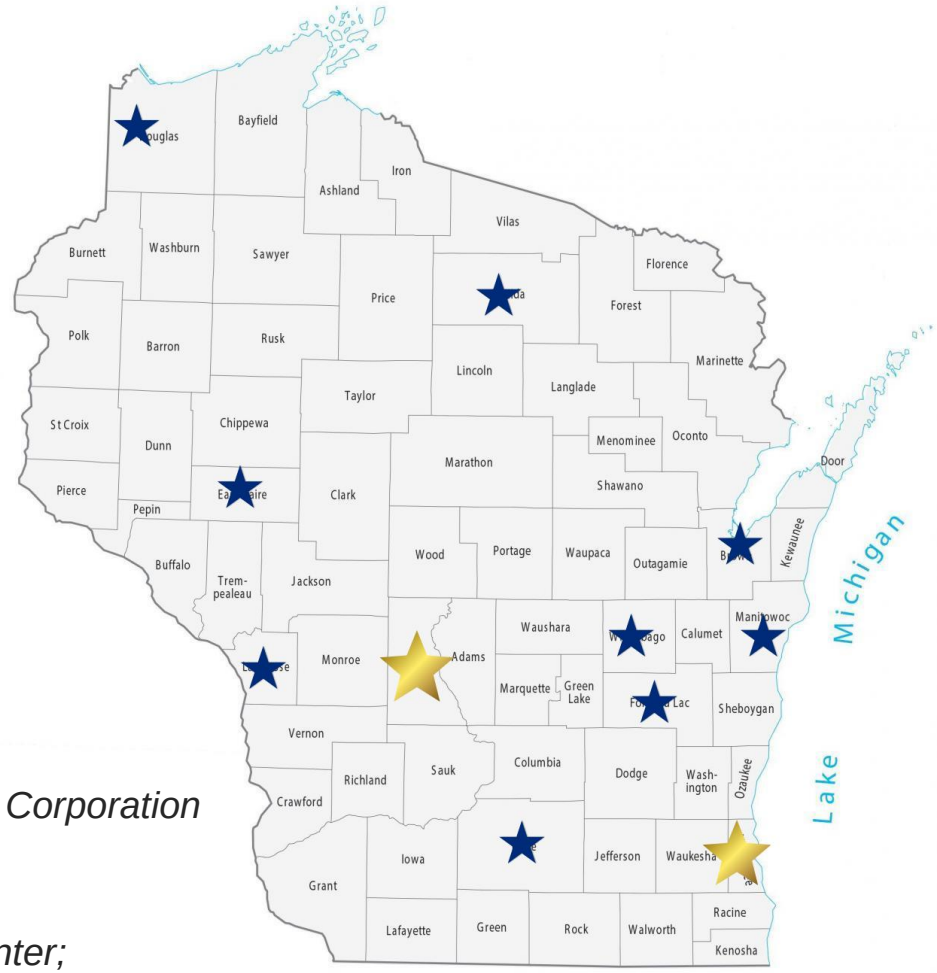
WPI provides services to all of Wisconsin's 72 counties

- 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……

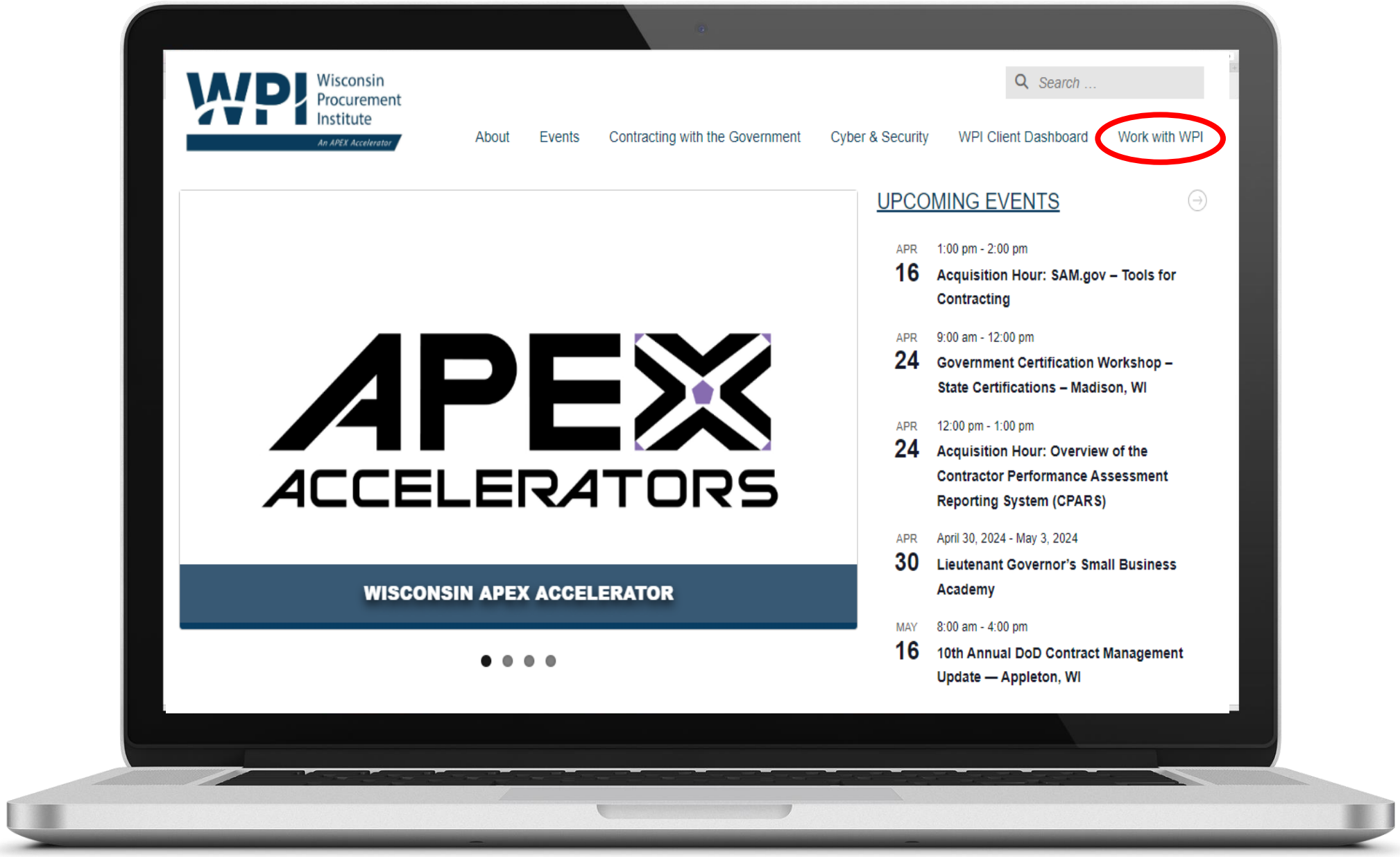
www.wispro.org

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*



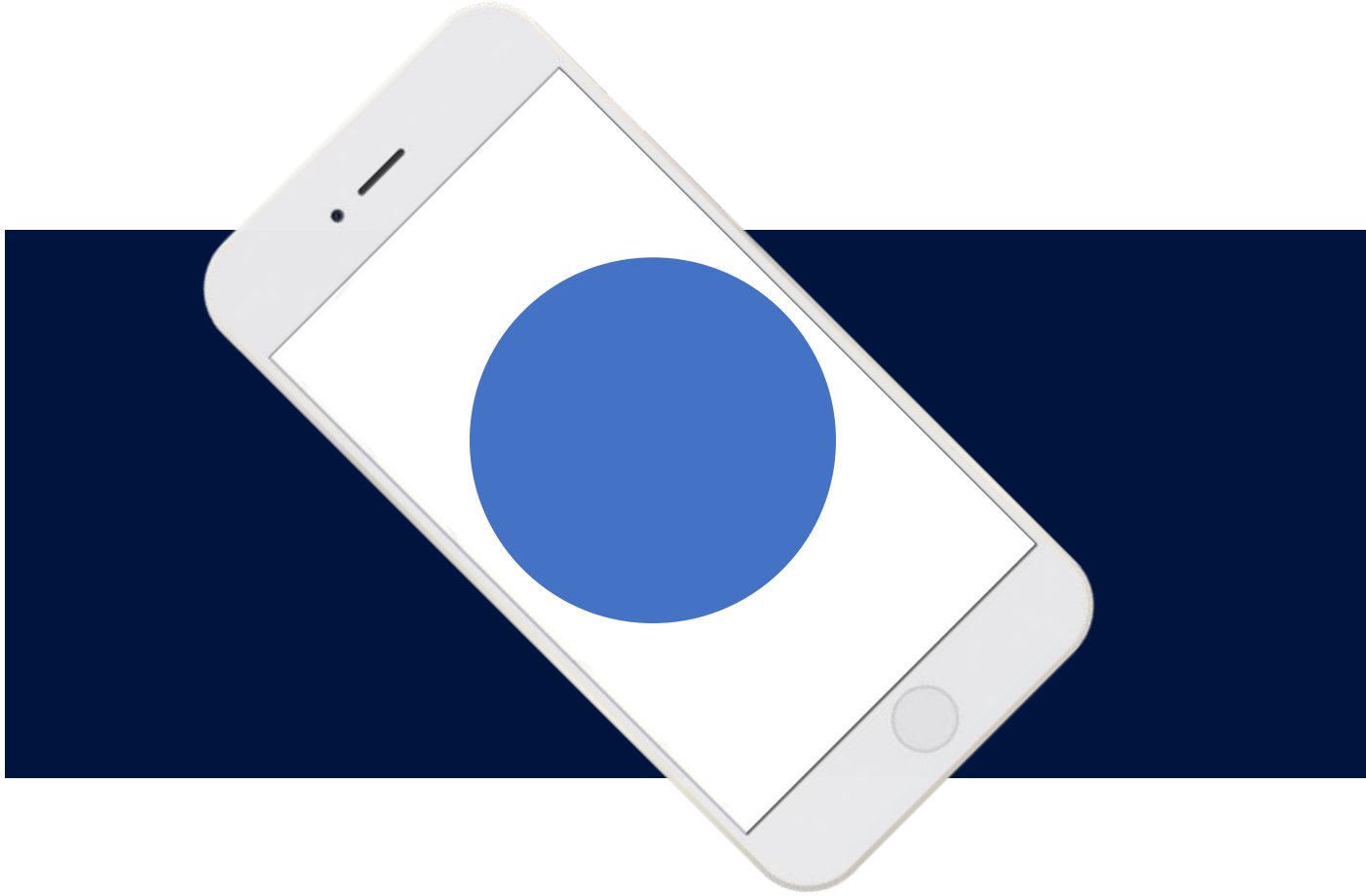
Wisconsin Procurement Institute
An APEX Accelerator


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 – September 20th, 2024

DFARS 252.204-7012

NIST
National Institute of Standards and Technology

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.

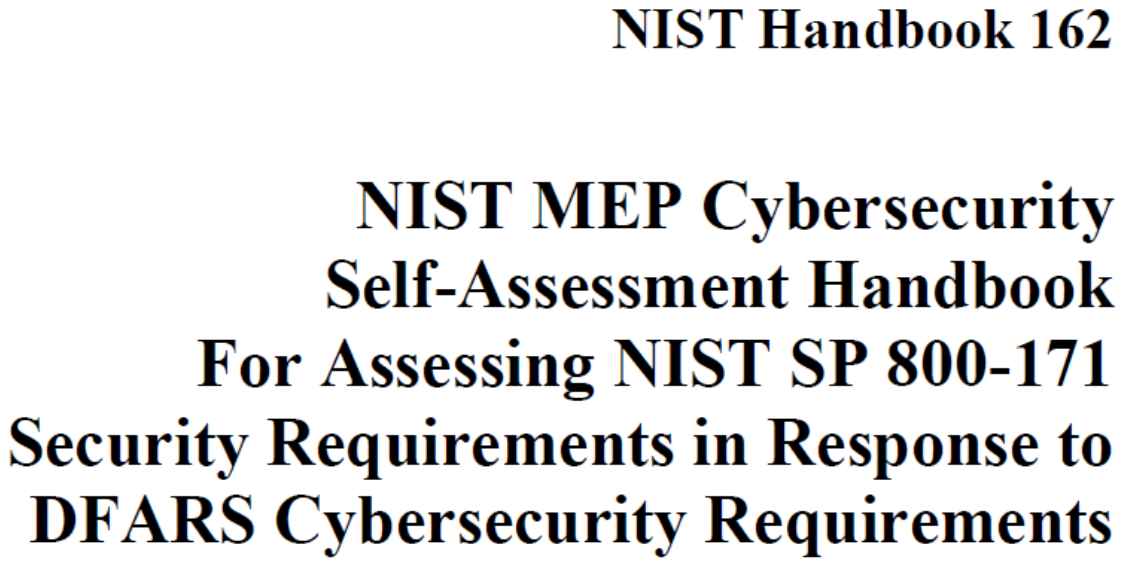
DFARS 252.204-7021

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



1 NIST Handbook 162

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

2 NIST SP 800-171A

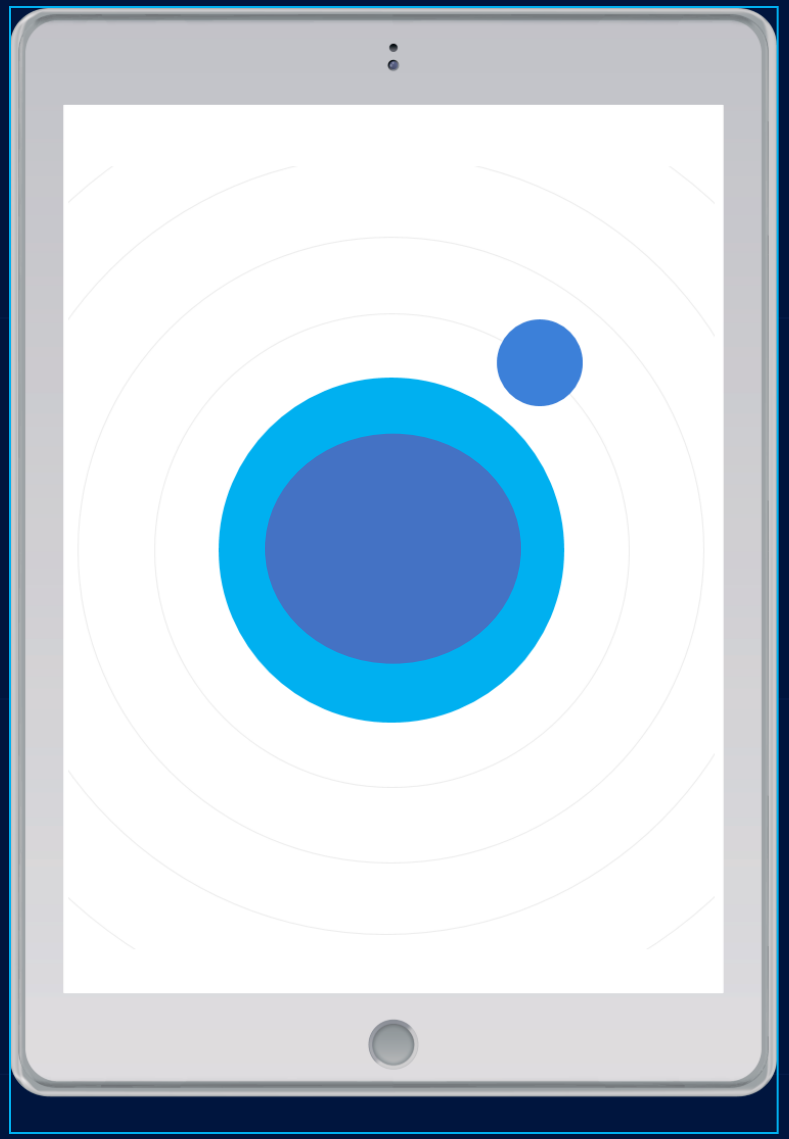
NIST Special Publication 800-171A
Assessing Security Requirements for Controlled Unclassified Information

3 NIST SP 800-18r1

NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans for Federal Information Systems

Elements of the Policy

1. Purpose
2. Scope
3. Policy Statement
4. Definitions
    1. Baseline Configuration
    2. Configuration Item
5. Roles and Responsibilities
    - Employees
    - Managers
    - Incident Response Team



Incident Response Team

Management

- ❑ Ownership and Authority
- ❑ Leadership and Delegation
- ❑ Accountability

IT Team Leader

- ❑ Technical Response
- ❑ Translating Concerns and Solutions
- ❑ Change Log and Incident Journal
- ❑ Forensic Assistance

Operations

- ❑ Business Continuity
- ❑ Customer Concern Response
- ❑ Incident Intelligence

Marketing & Legal

- ❑ Customer Communications
- ❑ Reporting Requirements
- ❑ Public Statements
- ❑ Liason with Law Enforcement

Prioritizing Incidents

Incident Prioritization Matrix

Urgency	Impact: High-System Wide Business Unit, Department, Location	Impact: Medium-Multiple Users Number of Users	Impact: Low-Single User Single User
High Can no longer perform primary work functions	**Critical**	**High**	**Moderate**
Medium Work functions impaired, the workaround in place	**High**	**Moderate**	**Low**
Low Inconvenient	**Moderate**	**Low**	**Low**

invgate

3.6.1	**SECURITY REQUIREMENT** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

ASSESSMENT OBJECTIVE

Determine if:

3.6.1[a]	*an operational incident-handling capability is established.*
3.6.1[b]	*the operational incident-handling capability includes preparation.*
3.6.1[c]	*the operational incident-handling capability includes detection.*
3.6.1[d]	*the operational incident-handling capability includes analysis.*
3.6.1[e]	*the operational incident-handling capability includes containment.*
3.6.1[f]	*the operational incident-handling capability includes recovery.*
3.6.1[g]	*the operational incident-handling capability includes user response activities.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records].

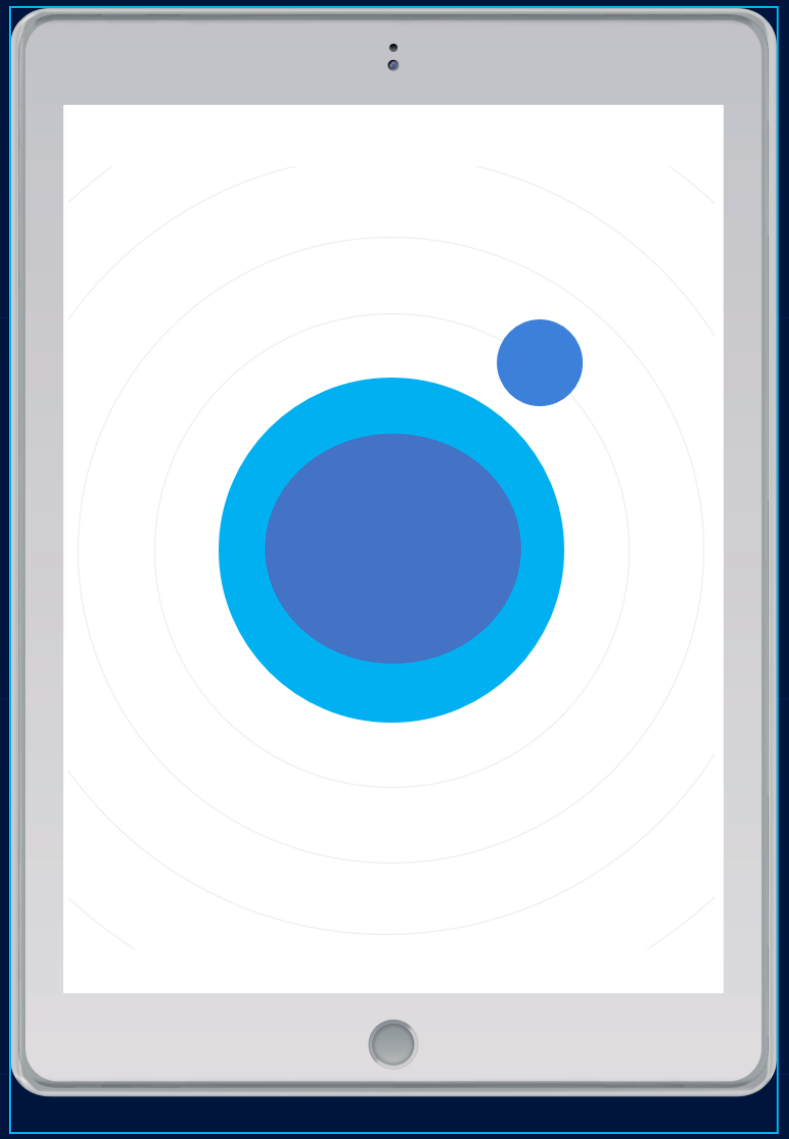
Interview: [*SELECT FROM:* Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support responsibilities; personnel with access to incident response support and assistance capability; personnel with information security responsibilities].

Test: [*SELECT FROM:* Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance].

Incident Response Stages & Procedures

Stage 1: Preparation
Stage 2: Detection
Stage 3: Containment
Stage 4: Investigation
Stage 5: Remediation
Stage 6: Recovery

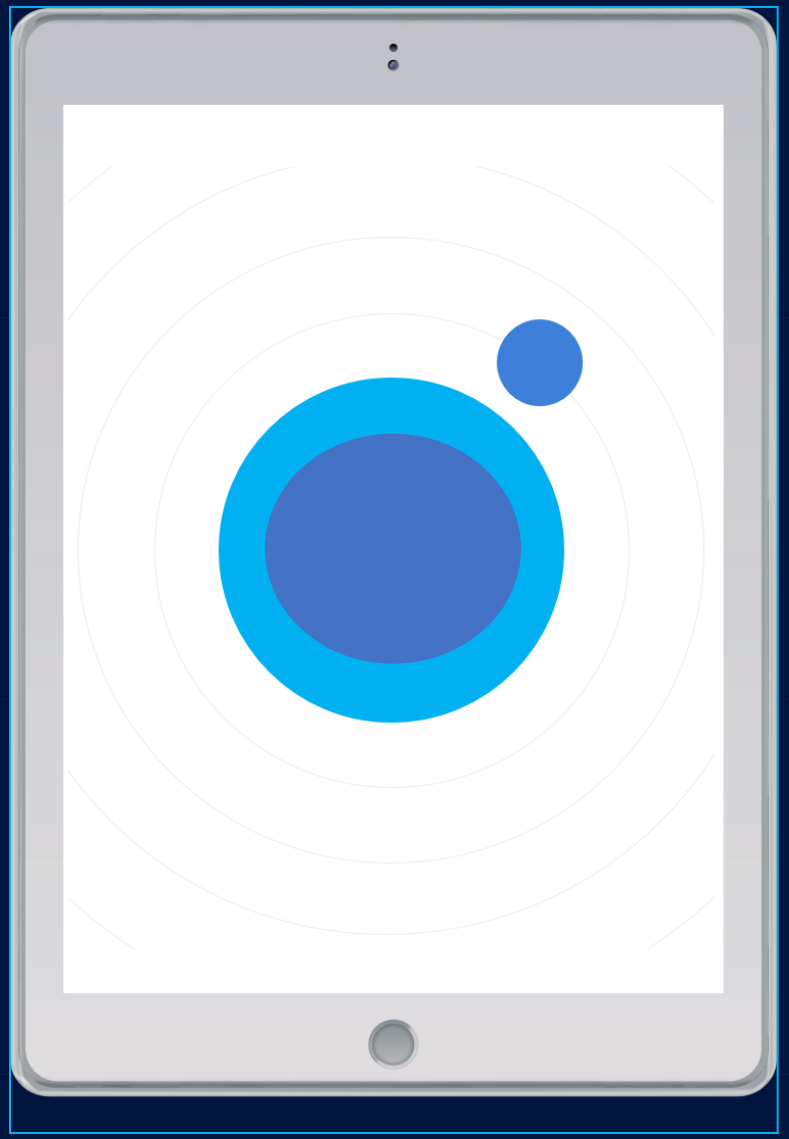
Elements of the Policy



PREPARATION

- Incident Response Team Foundation
- Documentation and Procedures Continuous Training
- Incident Detection Methods/Utilities
- 3rd Party Vendor Management Compliance Concerns

Elements of the Policy



Incident Response

3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.2[a]	*incidents are tracked.*
	3.6.2[b]	*incidents are documented.*
	3.6.2[c]	*authorities to whom incidents are to be reported are identified.*
	3.6.2[d]	*organizational officials to whom incidents are to be reported are identified.*
	3.6.2[e]	*identified authorities are notified of incidents.*
	3.6.2[f]	*identified organizational officials are notified of incidents.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

3.6.2 – Meeting The Controls

Incident Response Recording	
Incident Identification	• Record the date and time of the incident's discovery. • Document the source or method of detection (e.g., security alert, user report, system log). • Specify the affected systems, networks, or applications.
Incident Classification	• Document the nature and type of the incident (e.g., malware infection, unauthorized access). • Record the potential impact on critical assets, data, and operations. • Note the initial steps taken for containment and isolation. • Classify the incident severity (e.g., low, moderate, high) based on impact and threat level. • Specify the incident category (e.g., data breach, DDoS attack, insider threat).
Response Actions	• Document all actions taken to contain and mitigate the incident. • Record changes made to affected systems or configurations. • Specify tools, techniques, and procedures used for analysis and containment.
Communication Log	• Maintain a log of all internal and external communications related to the incident. • Document communication timestamps, recipients, and content discussed. • Note decisions made during communication with stakeholders. In the event these communications exist in digital record (such as email), please catalogue time and means of exchange for their reference.

Classifying Incidents

Incident Prioritization Matrix

Urgency	Impact: High-System Wide Business Unit, Department, Location	Impact: Medium-Multiple Users Number of Users	Impact: Low-Single User Single User
High Can no longer perform primary work functions	**Critical**	**High**	**Moderate**
Medium Work functions impaired, the workaround in place	**High**	**Moderate**	**Low**
Low Inconvenient	**Moderate**	**Low**	**Low**

invgate

3.6.2 – Meeting The Controls

Impact Assessment	• Document the extent of data or system compromise. • Record potential legal, financial, and reputational impacts. • Note the potential impact on stakeholders, customers, and partners.
Containment and Eradication	• Document the steps taken to contain the incident and prevent further spread. • Record actions to eradicate malware, close vulnerabilities, and remove unauthorized access. • Specify changes made to network configurations or access permissions.
Recovery Procedures	• Document the restoration process for affected systems and data. • Record validation steps to ensure systems are free from malware or vulnerabilities. • Note any additional security measures implemented post-incident.
Post-Incident Analysis	• Document lessons learned from the incident response process. • Record recommendations for improving incident response procedures. • Specify areas of the organization that require security awareness training or policy updates based on incident findings.
Reporting/Closure	• Document the resolution of the incident and the restoration of normal operations. • Prepare a detailed incident report outlining the incident, response actions, and lessons learned. • Specify any follow-up actions required and their respective deadlines.

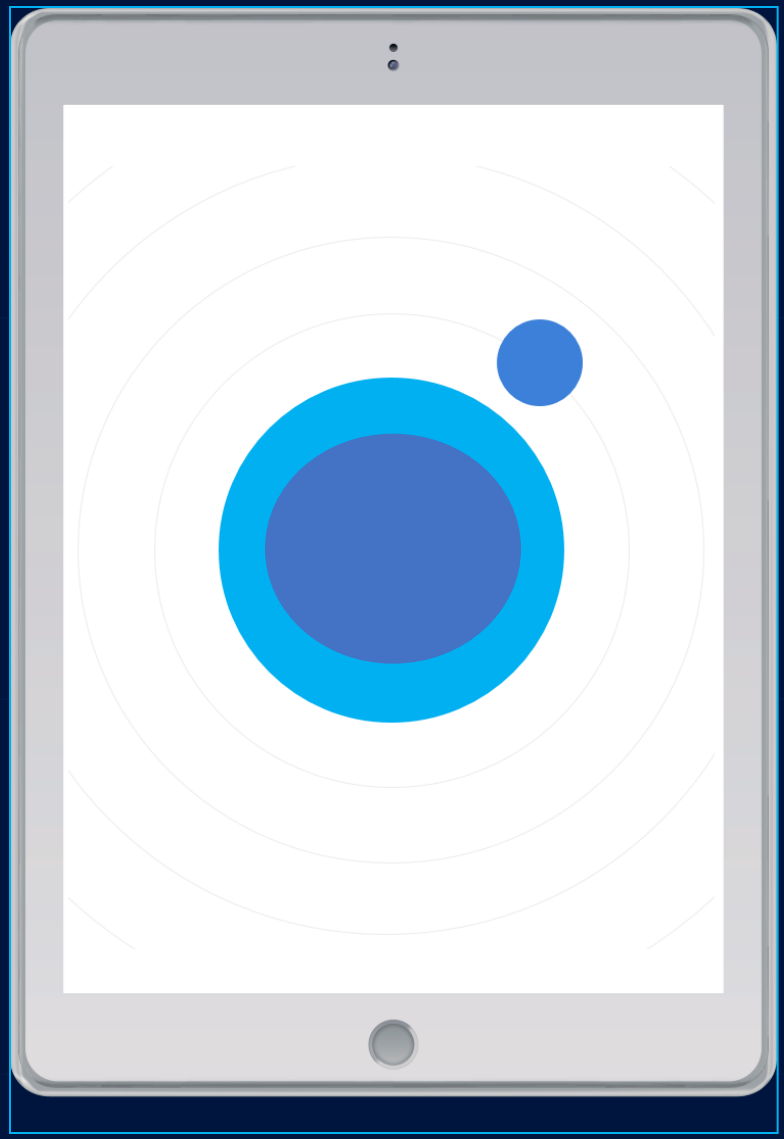
DETECTION

- **Real-Time Analysis**
- **Endpoint Detection & Response**
- **Incident Triage**

Detail the tools and processes you have. Particular technical requirements are not defined in this control set. Potential Tools already in-place could be:

Intrusion Detection (Firewall)
Antivirus
Remote Endpoint Management Tools

Elements of the Policy

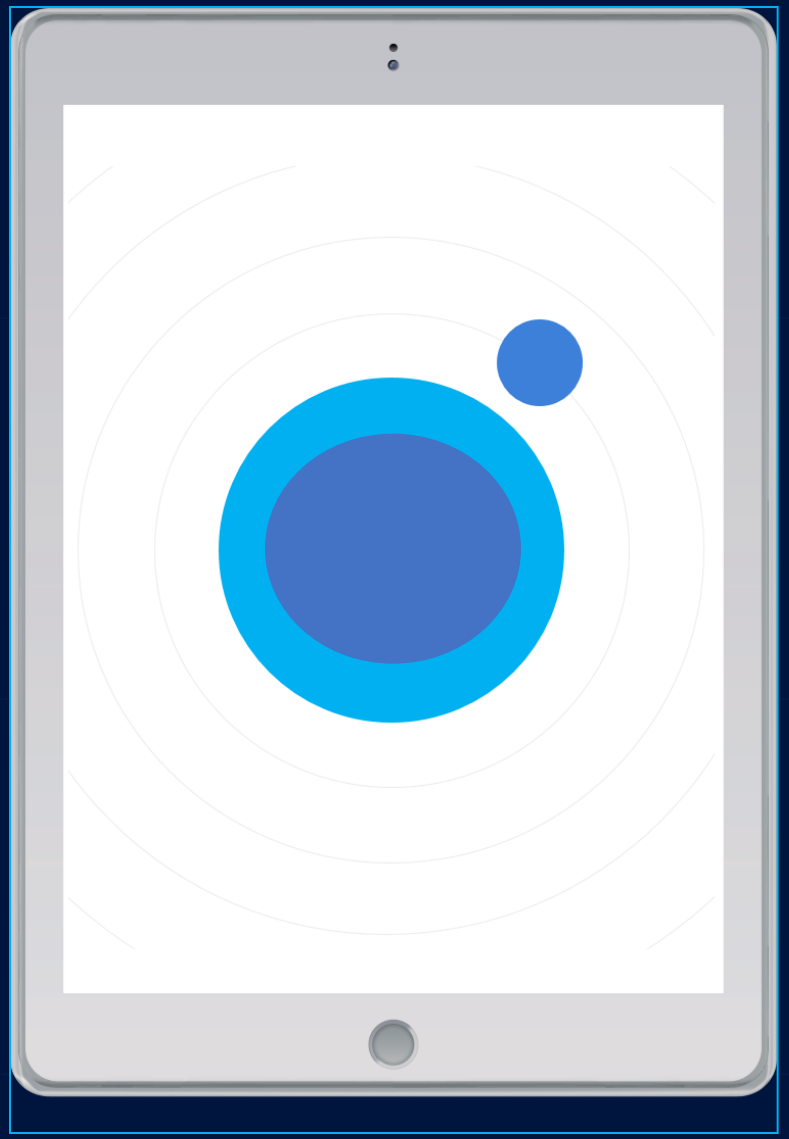


HOW CAN YOU HAVE AN ANOMALY IF YOU DO NOT HAVE CONSISTENCY?

CONTAINMENT

- Isolation(Quarantine)
- Account Management
- Access Control
- Patch & Vulnerability Management

Elements of the Policy



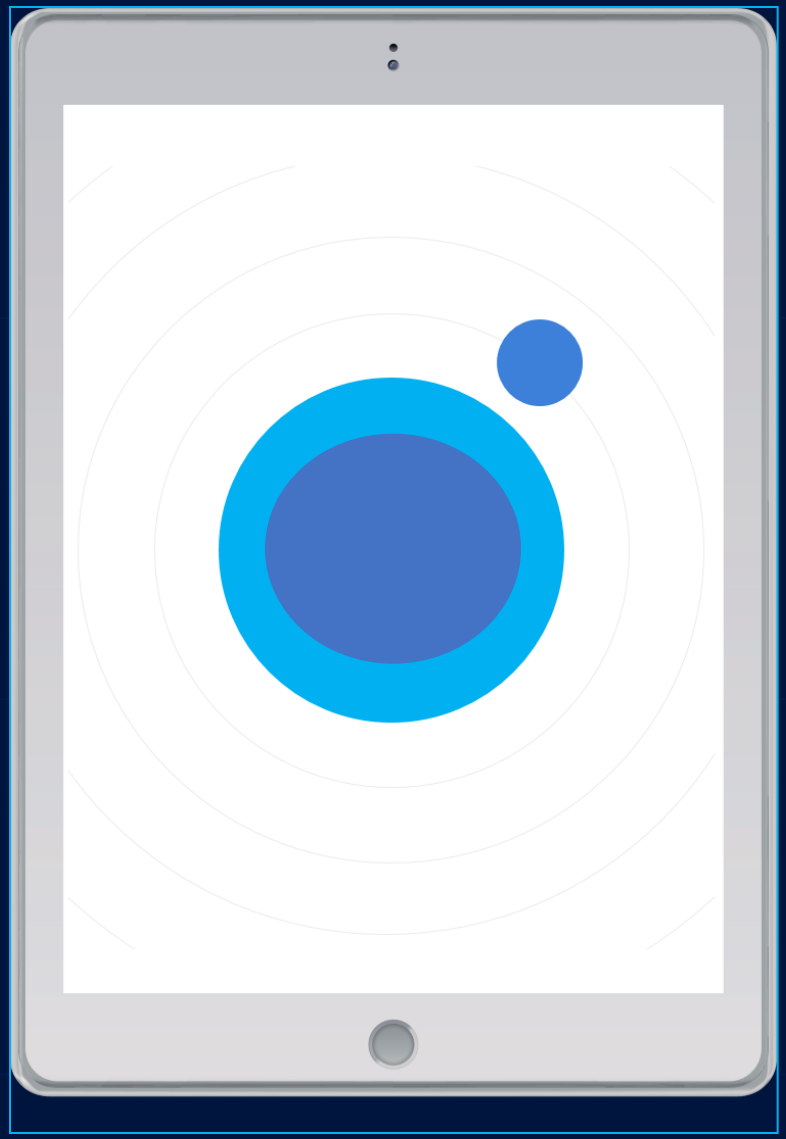
INVESTIGATION

- Cooperation with 3rd Party Providers
- Timeline Reconstruction
- Witness Interviews

Review Security Incidents thoroughly and document to the best of your ability. These efforts should contribute to the logging of the incident for review and future reference.

If utilizing 3rd party providers (particularly for managed services or security) – collaborate closely to try and determine a root cause of the incident.

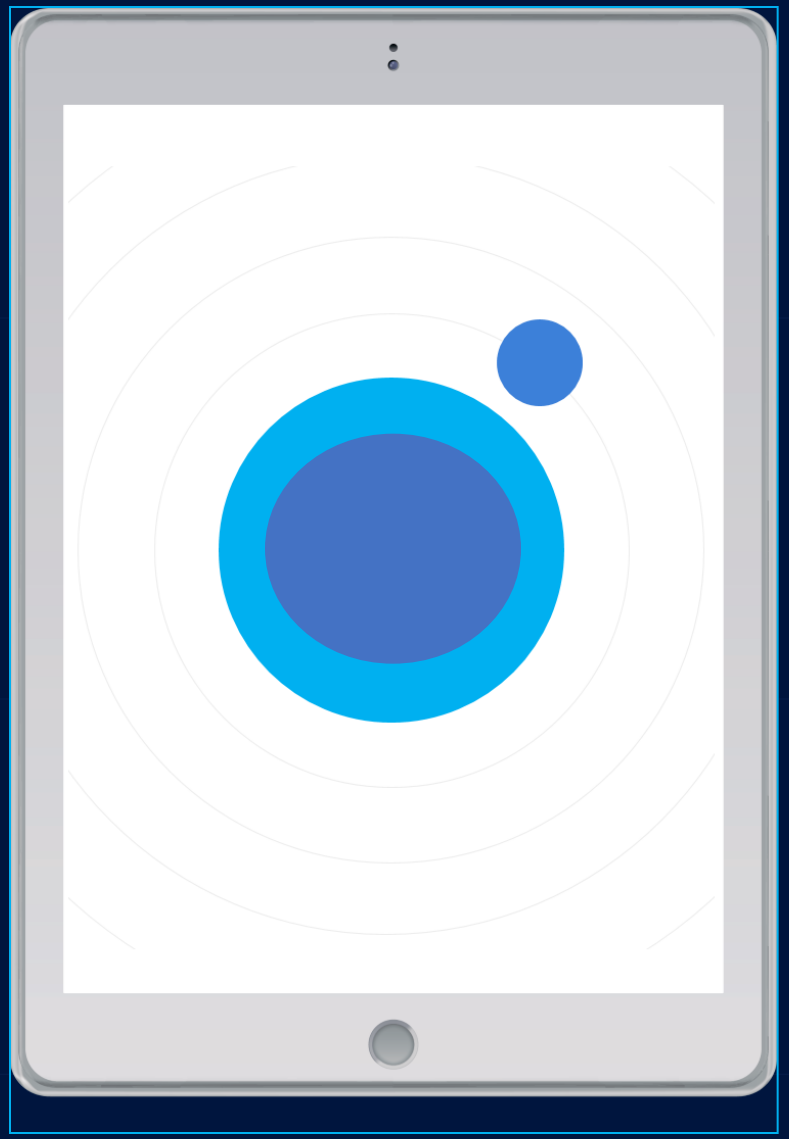
Elements of the Policy



REMEDIATION

- Backup and Recovery
- Patch Management
- Network Segmentation

Elements of the Policy



BACKUPS and BASELINES

What's a Backup?

Data Backup

[da·ta·back·up] **noun**

A copy or archive of your important information on a device.

The act of **backing up your data** is when you:

Create a copy of your important information.

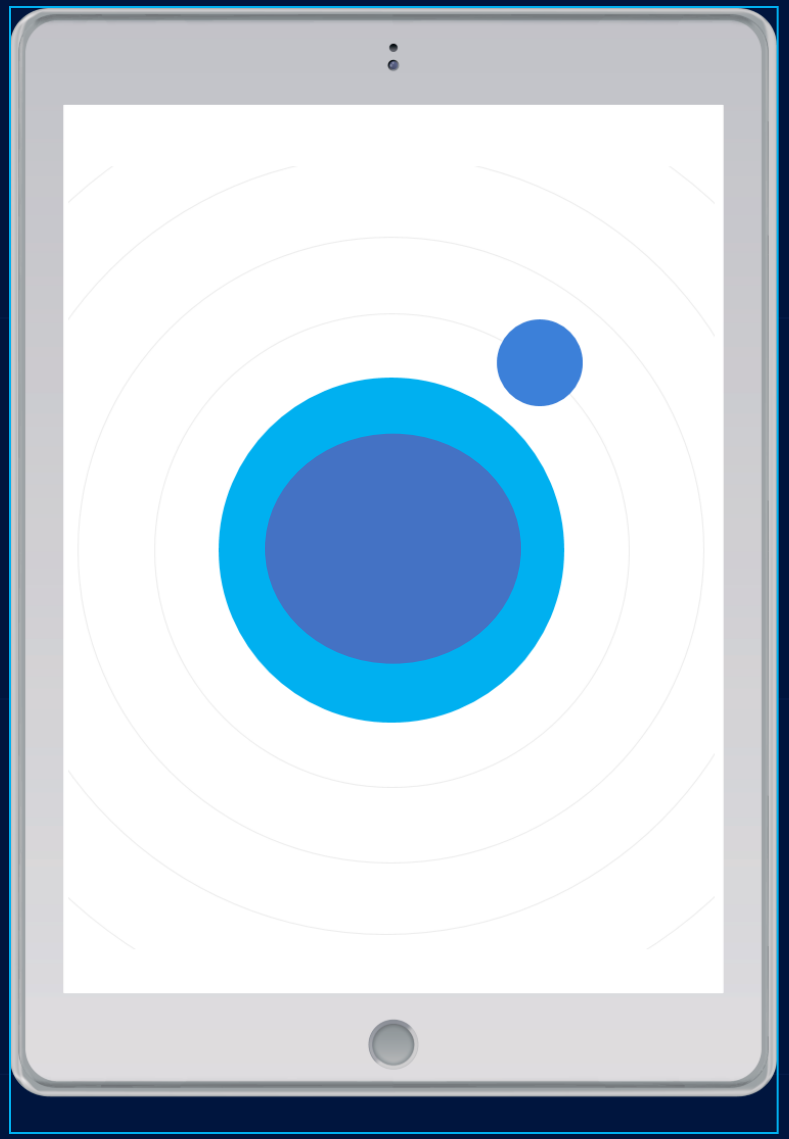
Store it in a secure, separate location.

Recognize the backup as a restoration method for your device.

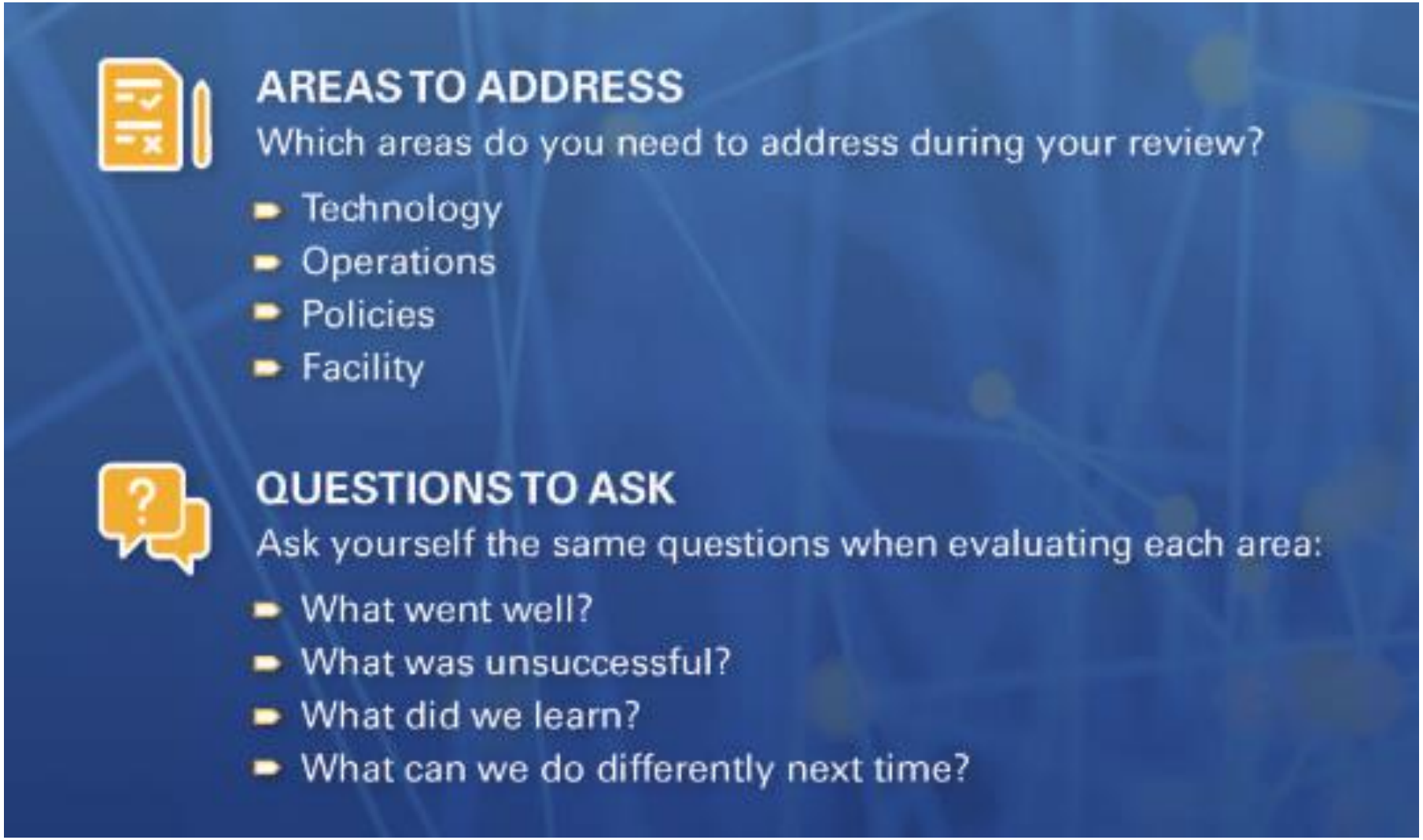
RECOVERY

- Return to Baseline
- Security Policy Review
- Incident Response Review
- Security Awareness Training

Elements of the Policy



Post-Incident Review

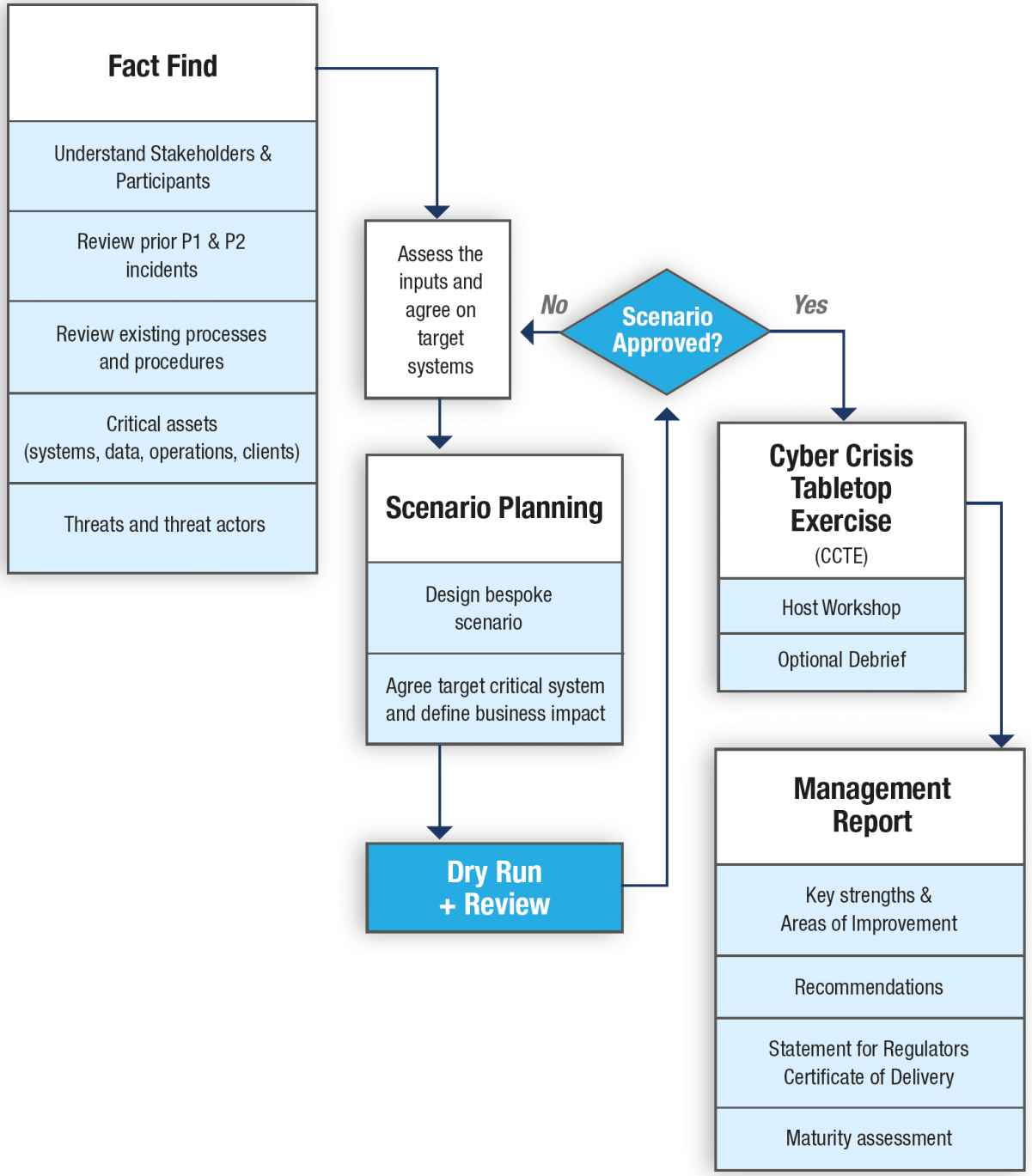


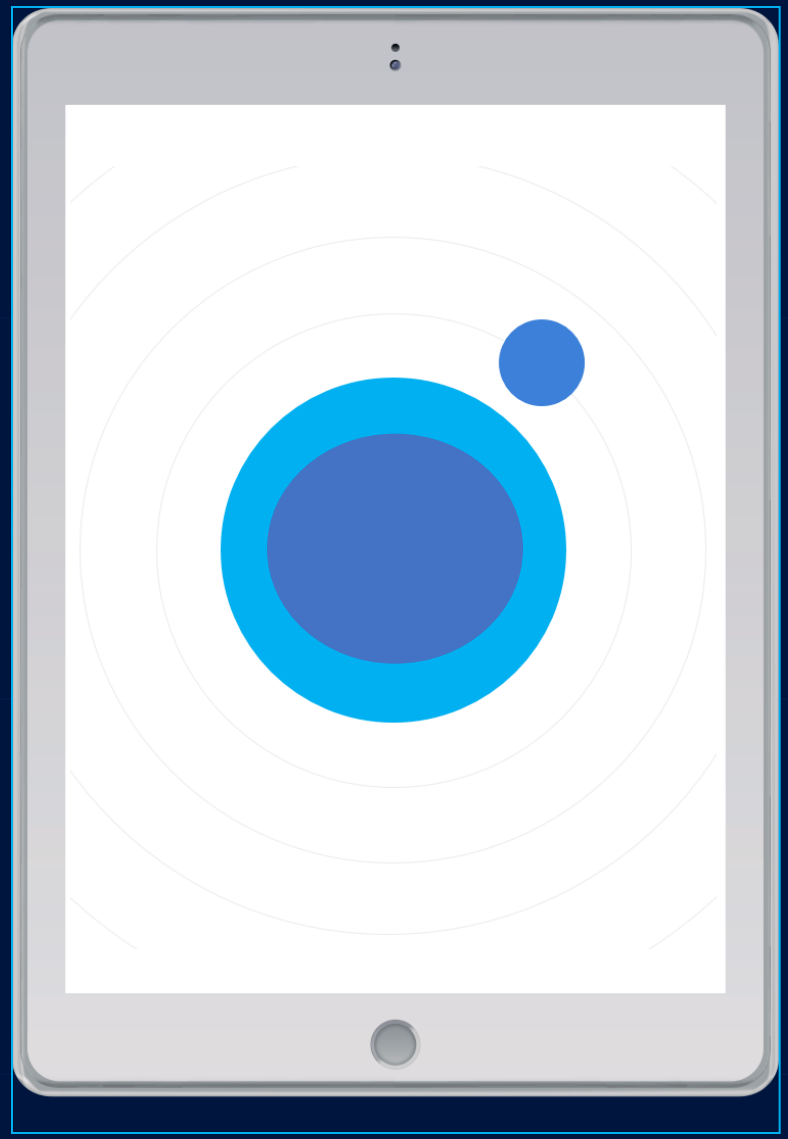
Post-Incident Review

Incident Response

3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	ASSESSMENT OBJECTIVE *Determine if the incident response capability is tested.*

Tabletop Exercisde



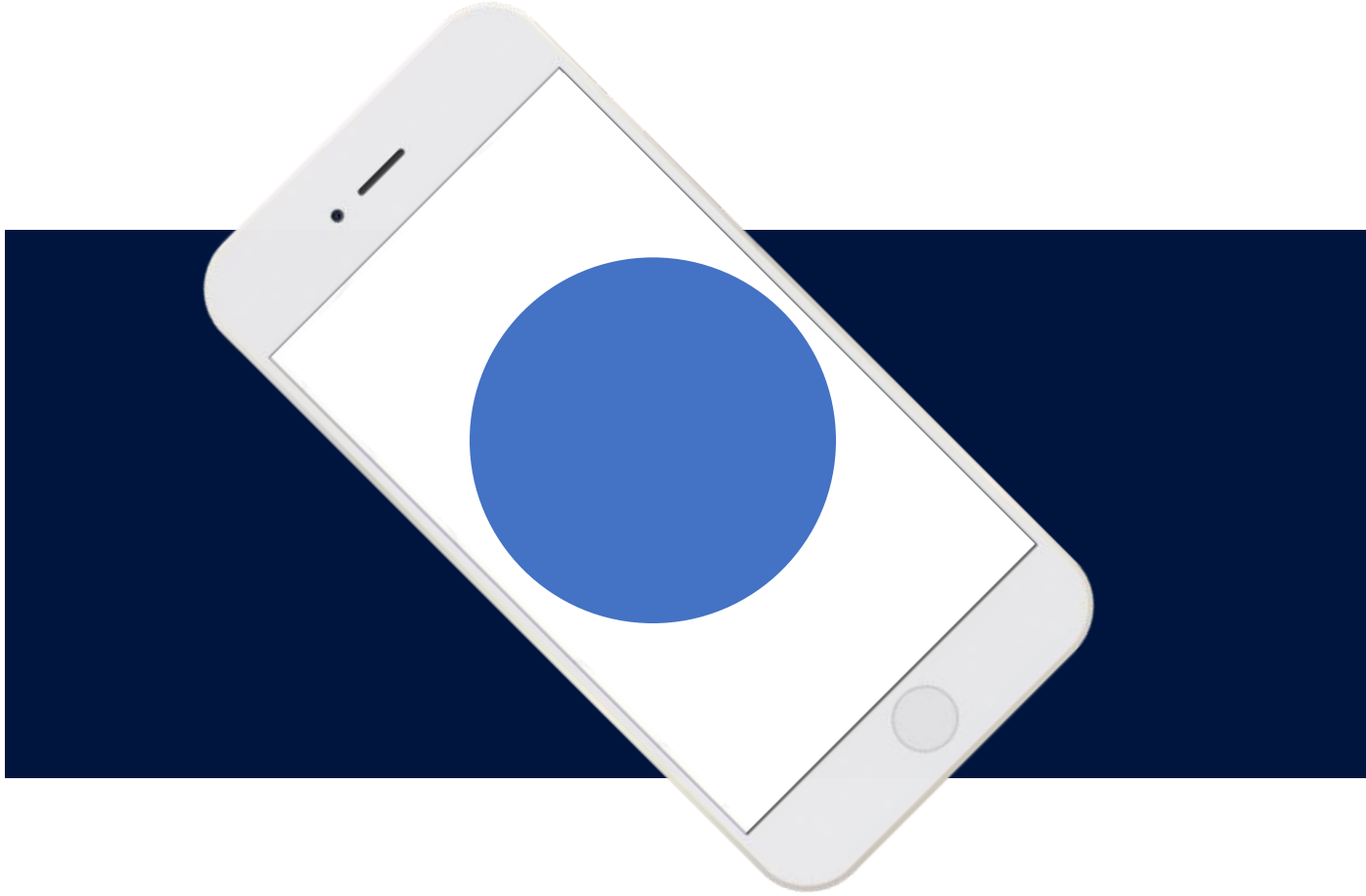


Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

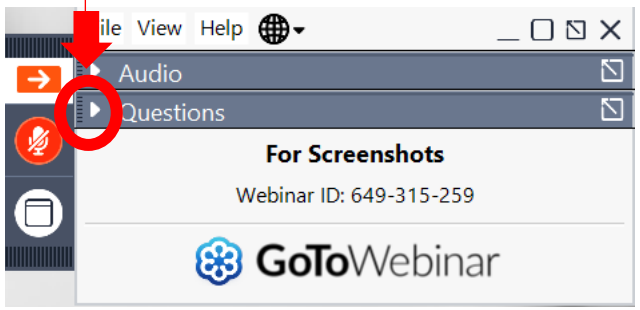
AN APEX ACCELERATOR



QUESTIONS?

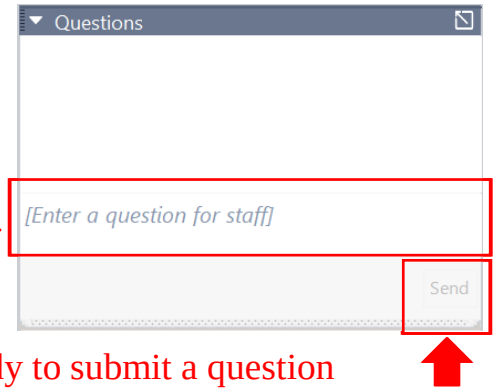
OPENING THE QUESTIONS BOX

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.

- **September 20,** 3.1.6 Incident Response Policy, Incident Response Plan
- **October 18,** 3.1.7 System Maintenance Policy
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- ~~**Aug 22 –** Regulation Making – The Process and the Important Role Businesses Play~~
- ~~**Sep 19 –** Industry 4.0 – The Next Generation of the DIB~~
- **Oct 24** – Innovation – What Does Innovation Look Like from DoD's Perspective?
- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

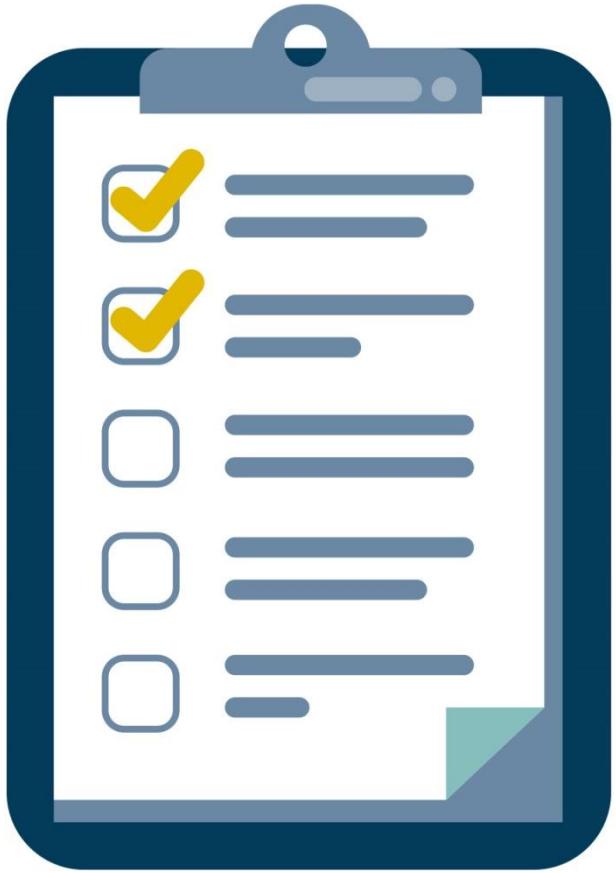
The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

September 20, 2024

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