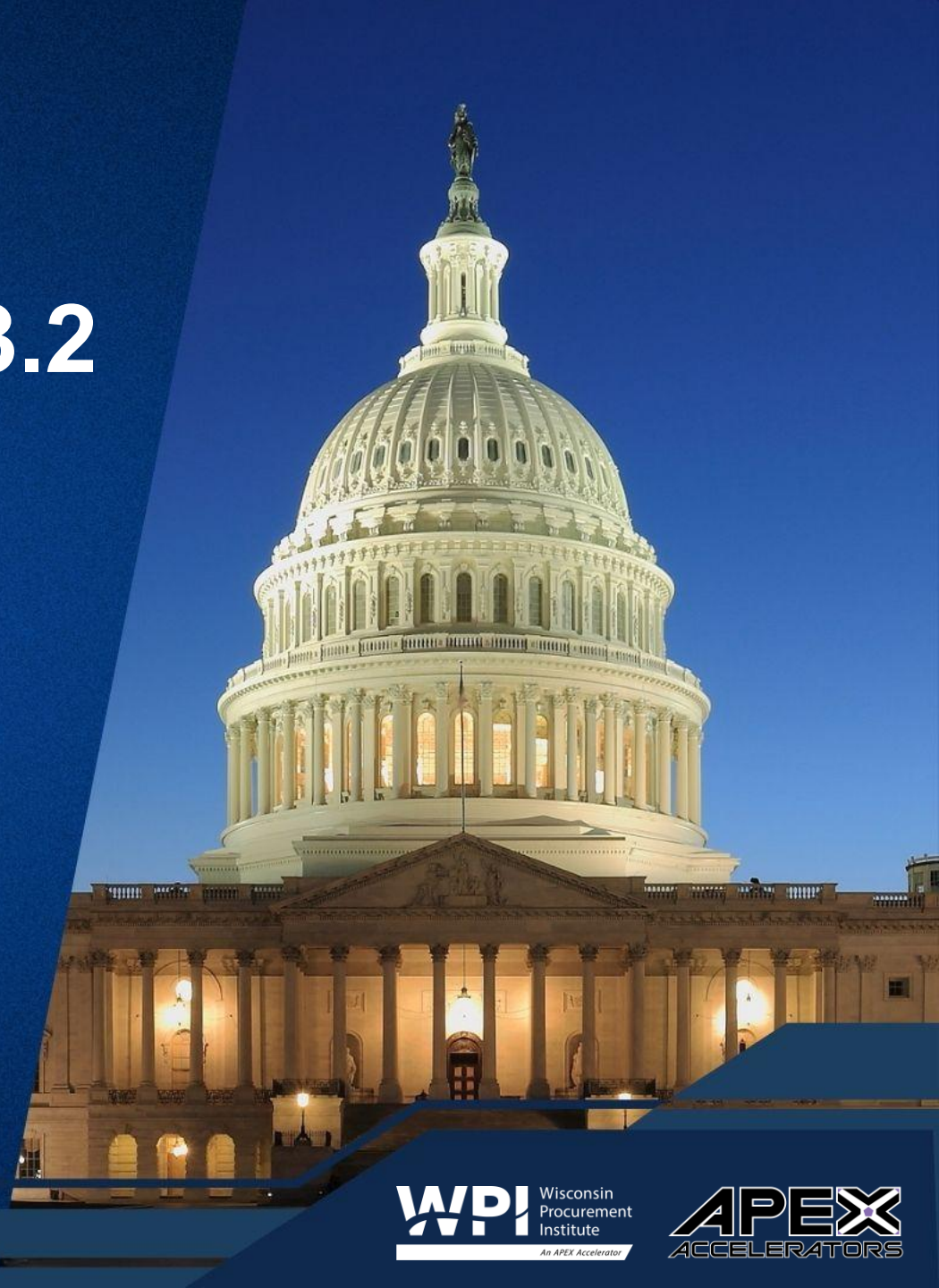
Cyber Thursday:

CMMC: Control Set Series: 3.2 Awareness and Training

March 26| 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute



Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

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.

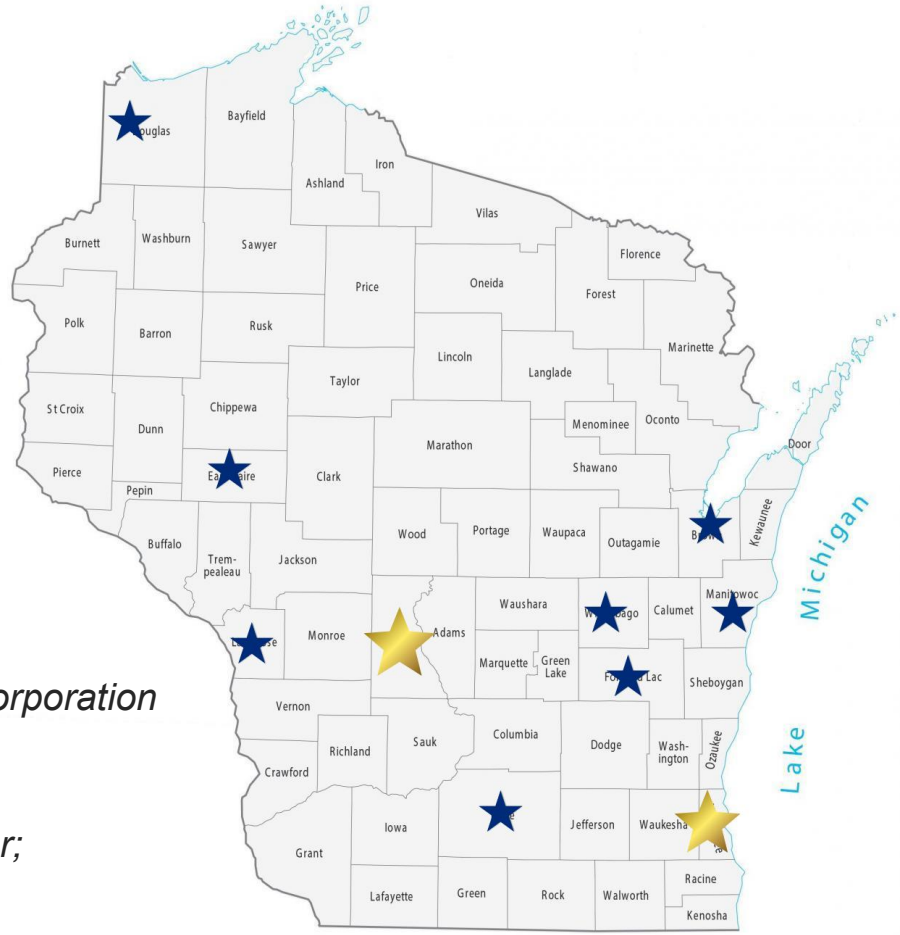
WPI provides services and training to all of Wisconsin's 72 counties

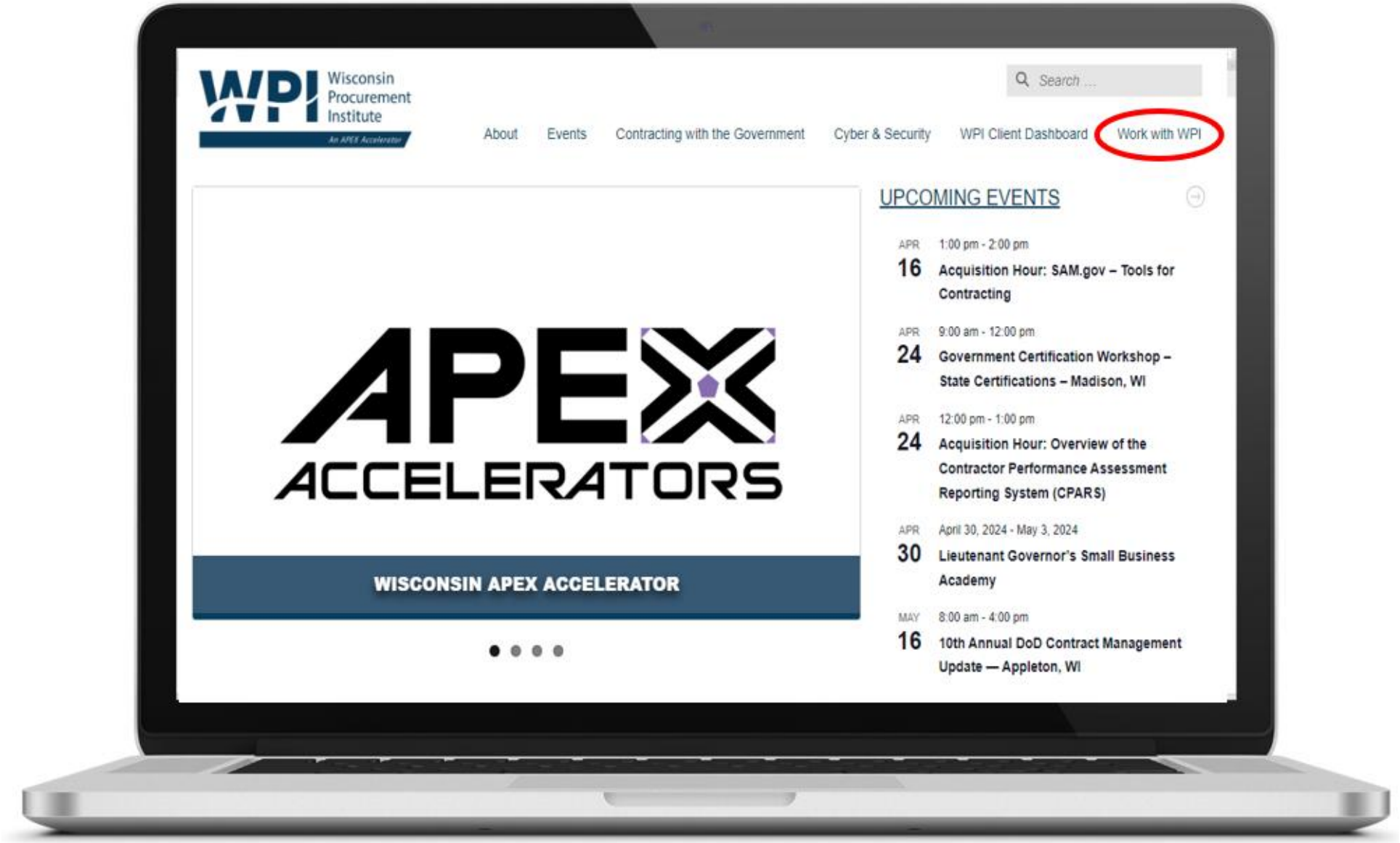
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *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*

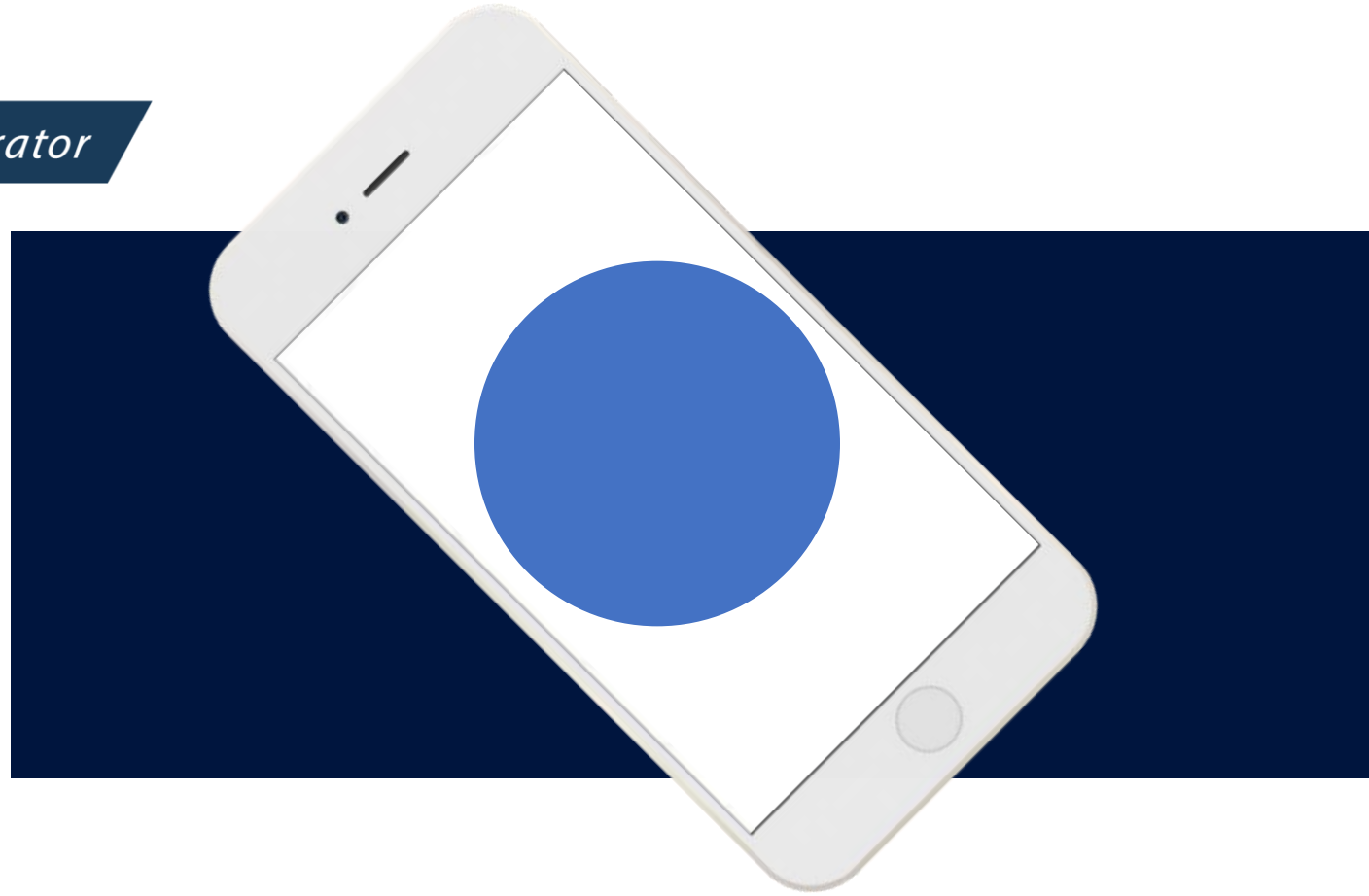



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 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

Wisconsin Procurement Institute

An APEX Accelerator

Access Control



Cyber Thursday – March 26th, 2026


LOCKHEED MARTIN
3103

14 Families – 110 Controls – 320 Audit Objectives

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

ABOUT US ▾ ACCREDITATION ▾ RESOURCES ▾ CMMC ECOSYSTEM ▾ NEWS & EVENTS ▾ MARKETPLACE CAICO

www.cyberab.org

CMMC Assessment Guide

Level 2

Version 2.0 | December 2021

1. CMMC Assessment Guide (Level 2)
2. NIST Special Publication 800-171A
   Assessing Security Requirements for
   Controlled Unclassified Information
3. DoD Memo
   DoD Guidance for Reviewing System
   Security Plans and the NIST SP 800-
   171 Security Requirements

AT.L2-3.2.1 – ROLE-BASED RISK AWARENESS

Ensure that managers, systems 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.

ASSESSMENT OBJECTIVES [NIST SP 800-171A][56]

Determine if:

[a] security risks associated with organizational activities involving CUI are identified;

[b] policies, standards, and procedures related to the security of the system are identified;

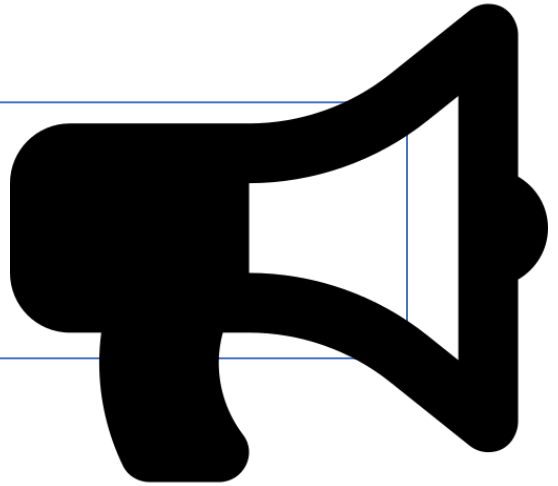
[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities; and

[d] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems 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.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.1[a] *security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b] *policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c] *managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d] *managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].

DOMAIN 3.2 · CONTROL AT.L2-3.2.1

Role-Based Risk Awareness



Ensure everyone knows the risks and the rules

AT.L2-3.2.1 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Ensure that managers, systems 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.

ASSESSMENT OBJECTIVES — All four must be MET:

[a]	Security risks associated with organizational activities involving CUI are identified.
[b]	Policies, standards, and procedures related to the security of the system are identified.
[c]	Managers, systems administrators, and users are made aware of the security risks associated with their activities.
[d]	Managers, systems administrators, and users are made aware of the applicable policies, standards, and procedures related to system security.

AT.L2-3.2.1 –

SECURITY REQUIREMENT

Security risks associated with organizational activities involving CUI are identified.

ASSESSMENT OBJECTIVES — All four must be MET:

1	What risks, and why do you feel they are risks, are present to your organization?
2	How are these risks regularly communicated with employees?
3	Can you (and do you) have a way of measuring the impact of this training on user behavior?

Control Requirements

Synchronous Training

- Live Webinars (Hi, Hello!)
- Real-Time Phishing Exercises
- In-Person Workshops or Sessions

Asynchronous Training

- Self-Paced Training Modules
- Interactive Simulations
- Quizzes and Knowledge Checks
- Notices and Alerts (email, etc.)

Annual/Regular Considerations

- Onboarding
- Annual
- Phishing Campaigns and Educational Notices

AT.L2-3.2.1 – How to Implement: Building Your Awareness Program

Step 1: Identify Your Risks & Policies

- Document the specific CUI security risks in your environment (e.g., data exfiltration, phishing, accidental disclosure)
- Identify all policies, standards, and procedures employees must follow
- Map risks and policies to the roles in your organization

Step 2: Build Your Awareness Training

- Create or procure a formal training curriculum covering: CUI handling, phishing recognition, password hygiene, acceptable use
- Training can be synchronous (live sessions) or asynchronous (online modules)
- Simulated phishing campaigns count as awareness techniques — run them regularly

Step 3: Deliver to All Required Personnel

- Training must reach: all users, managers, and systems administrators with access to in-scope systems
- Conduct initial training for new employees before granting system access
- Conduct periodic refresher training — at least annually, per CMMC's definition of 'periodically'

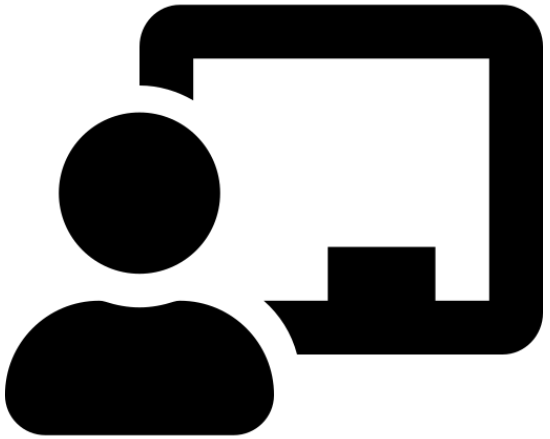
Step 4: Document & Track Everything

- Use a Learning Management System (LMS) or training tracker to log completions
- Retain training records — completion dates, employee names, course titles
- Keep training materials, curricula, and policies in final approved form

DOMAIN 3.2 · CONTROL AT.L2-3.2.2

Role-Based Training

Tailored training for personnel with security responsibilities



AT.L2-3.2.2 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Ensure that personnel are trained to carry out their assigned information security responsibilities.

ASSESSMENT OBJECTIVES — All three must be MET:

[a]	Individual information security responsibilities are identified for each role that requires role-based security training.
[b]	Role-based security training is provided before allowing access to the system, CUI data, or performing assigned security duties.
[c]	Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.

AT.L2-3.2.2 – Who Needs Role-Based Training?

The CMMC L2 Assessment Guide lists specific roles that must receive security-related technical training tailored to their assigned duties. This goes beyond general awareness — each role's training must address the specific risks and responsibilities of that job.

System / Network Administrators

Require training on: secure configuration management, patch management, account lifecycle management, firewall/network controls, audit log review

Security Personnel / CISOs

Require training on: security assessment methods, incident response procedures, risk assessment, CMMC control requirements, POA&M management

Configuration Managers / Change Control

Require training on: authorized change procedures, security impact analysis, access restrictions for change, audit trail requirements

Auditors / Compliance Personnel

Require training on: audit log review, evidence collection, CMMC assessment methodology, documentation requirements, reporting obligations

Software / System Developers

Require training on: secure coding practices, security architecture requirements, CUI handling in development, system integration security

Procurement / Contracting Personnel

Require training on: CUI flow-down requirements, DFARS clauses, subcontractor security obligations, contract data handling requirements

AT.L2-3.2.2 – Evidence & How to Prove It

Evidence You Must Gather

Examine	Role-based training policy and curriculum for each security role
Examine	Training records showing completion before system access was granted
Examine	Job descriptions or role definitions documenting security responsibilities
Examine	LMS exports mapping employees to their specific role-based courses
Interview	Ask a sysadmin: 'What training did you receive before being given admin rights?'
Interview	Ask a security manager: 'How is training content determined for your role?'
Test	Demonstrate the LMS showing role assignments, course enrollment, and completions
Test	Show new-hire onboarding process includes role-based training before access is provisioned

Common Failure Points to Avoid

No role mapping

General awareness training given to sysadmins instead of role-specific technical training. ALL in-scope roles must have tailored curricula.

Late training

Training records show training was completed after system access was granted. Must be before access. Check your new-hire provisioning workflow.

No documentation of responsibilities

You provide training but have no documented list of what security duties each role performs. Objective [a] requires this to be written down.

Relying on vendor training alone

Vendor product training doesn't automatically satisfy CMMC role-based training. Content must map to YOUR security responsibilities.

Training materials in draft

If your course materials or policy are marked 'DRAFT', they are not acceptable evidence. Everything must be finalized and approved.

DOMAIN 3.2 · CONTROL AT.L2-3.2.3

Insider Threat Awareness

Train your people to recognize and report threats from within

AT.L2-3.2.3 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

ASSESSMENT OBJECTIVES — Both must be MET:

[a]	Potential indicators of insider threat are identified. Your training must be based on identified, documented threat indicators — not just a vague mention of 'insider threats'.
[b]	Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Important note from the Assessment Guide:

This control does NOT require a separate standalone insider threat training module. Insider threat content may be embedded within your existing security awareness training program (3.2.1), as long as it clearly addresses recognition and reporting of insider threat indicators.

AT.L2-3.2.3 – What Your Training Must Cover

The CMMC L2 Assessment Guide specifies the behavioral indicators your training must address. Your training content must be based on identified, documented indicators — vague references won't satisfy objective [a].

Indicators Your Training Must Include (per CMMC Guide)

- Inordinate or long-term job dissatisfaction
- Attempts to access information not required for job performance
- Unexplained access to financial resources
- Bullying or sexual harassment of fellow employees
- Workplace violence or threats
- Serious violations of organizational policies, directives, or procedures
- Unusual after-hours access or work patterns outside normal schedules
- Excessive downloading or copying of sensitive data

Managers: Focus On

- Observing team members for behavioral changes
- Understanding normal work patterns to identify anomalies
- Reporting channels and procedures for concerns
- Documenting observations per policy

Employees: Focus On

- General behavioral indicators visible in the workplace
- How to report concerns to management or HR
- Understanding they are not expected to investigate — only report
- Anonymity and non-retaliation policies

AT.L2-3.2.3 – Evidence & Assessment Considerations

Objective	Examine (Documents to Gather)	Interview (Questions to Prepare)	Test (Mechanisms to Demo)
[a]	Documented list of insider threat indicators used as basis for your training content; threat intelligence sources reviewed	How did you determine which indicators to include in your training? Where is this documented?	Show the documented indicator list in your SSP or training development records
[b]	Training curriculum showing insider threat content; LMS records of completion for managers AND employees; training materials (final form)	Ask a manager: 'What indicators would cause you to report a concern?' Ask an employee: 'How do you report a potential insider threat?'	Demo training platform showing insider threat module; show completion records for all in-scope staff

Practical Implementation Options for 3.2.3:

- Add a dedicated "Insider Threat" module to your existing LMS security awareness course — this works to satisfy both 3.2.1 and 3.2.3 simultaneously
- Use CISA's free Insider Threat Awareness training materials (ciisa.gov) as a starting point — document them in your SSP
- Reference NIST SP 800-53 Section PS (Personnel Security) and law enforcement bulletins to document your indicator list for objective [a]
- Ensure reporting mechanism is explicitly addressed in training (HR hotline, supervisor escalation path, anonymous tip line, etc.)

Readiness Checklist — AT.L2-3.2.1

AT.L2-3.2.1
Role-Based Risk Awareness

Everyone with access to in-scope systems must be trained. Check every item before your C3PAO arrives.

- [ ] 1 **CUI security risks documented**
  Risk register, SSP risk section, or standalone CUI risk documentation — must be in final, approved form
- [ ] 2 **Security awareness policy finalized and approved**
  Acceptable use policy also required; drafts do not count as evidence
- [ ] 3 **Training curriculum developed and covers risks + policies**
  Content must address CUI risks, phishing, password hygiene, acceptable use, and incident reporting
- [ ] 4 **Training delivered to ALL in-scope users, managers, and sysadmins**
  Everyone with access to systems that process, store, or transmit CUI must be included
- [ ] 5 **Training completion records on file**
  LMS completion exports, signed attendance sheets, or equivalent — names, dates, course titles
- [ ] 6 **Refresher training scheduled at least annually**
  'Periodically' in CMMC means no longer than 12-month intervals; document your schedule
- [ ] 7 **Staff can articulate security risks and where policies are located**
  Interview readiness: assessors will ask your employees and managers directly — prepare them

✓ **Key evidence bundle: training policy (final) + LMS completion report + signed acceptable use policy covers most of 3.2.1**

Readiness Checklist — AT.L2-3.2.2

AT.L2-3.2.2
Role-Based Training

Personnel with security duties need deeper, role-specific training — not just the general awareness program.

- [ ] 1 **Security roles and responsibilities formally documented**
  Job descriptions, role matrix, or SSP section listing security duties per role
- [ ] 2 **Role-specific training curricula developed for each security role**
  Covers: sysadmins, security staff, config managers, auditors, developers, procurement — each needs tailored content
- [ ] 3 **Training provided BEFORE system access was granted**
  Critical timing requirement: new-hire onboarding must include role-based training prior to access provisioning
- [ ] 4 **LMS shows role-based course assignments and individual completions**
  Assessors need to see who took which role-specific course and when — not just general training completions
- [ ] 5 **Personnel in security roles can describe their duties and training received**
  Interview readiness: sysadmins should articulate what security-specific training they received before being given admin rights
- [ ] 6 **Training content maps to actual security duties in your environment**
  Recommended: reference NIST SP 800-181 NICE work roles to document knowledge and skills required per role

✓ **Key evidence bundle: role-responsibility matrix + role-specific curricula + LMS showing pre-access completion per employee**

Readiness Checklist — AT.L2-3.2.3

AT.L2-3.2.3

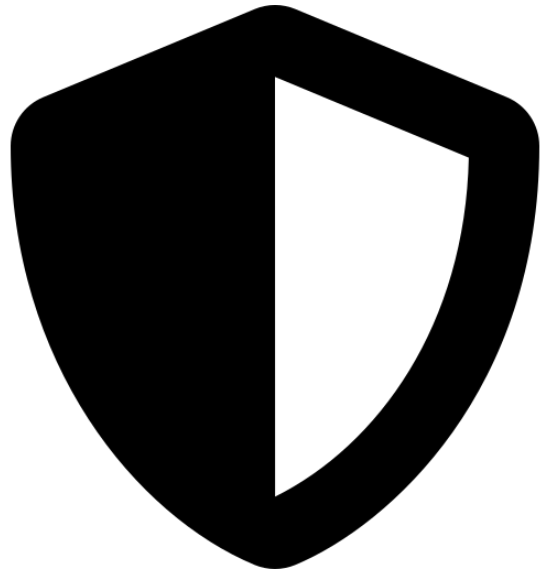
Insider Threat Awareness

Both managers AND employees must be trained. Content can be embedded within your 3.2.1 program — no separate module required.

- [ ] 1 **Insider threat indicators formally identified and documented**
  Objective [a]: your training content must be based on a written list of indicators; vague references are not sufficient
- [ ] 2 **Training curriculum includes insider threat recognition and reporting**
  Can be a module within your 3.2.1 awareness program — does not need to be a standalone course
- [ ] 3 **Manager-specific content addresses behavioral observation**
  Managers need guidance on recognizing team member behavior changes and proper escalation procedures
- [ ] 4 **Employee content covers reporting procedures and general indicators**
  Employees need to know what to report, how to report it, and that non-retaliation protections exist
- [ ] 5 **Reporting mechanism explicitly covered in training**
  Must name the actual channel: HR hotline, supervisor escalation, anonymous tip line, etc.
- [ ] 6 **All in-scope managers AND employees have completed training — records on file**
  Both groups required; LMS must show completion records for each; assessors will verify coverage

✓ **Key evidence bundle: documented indicator list + training curriculum showing insider threat module + completion records for all staff**

Key Takeaways



- Domain 3.2 is a people problem as much as a technology problem — it requires documented, delivered, and proven training programs
- 3.2.1 covers everyone; 3.2.2 requires deeper role-specific training; 3.2.3 adds insider threat content — all three must be MET
- Evidence must be final and approved: records, curricula, policies, and LMS data are your primary artifacts
- Start building your training program now — C3PAO assessment lead times are 9–12 months and growing

KEY REFERENCES

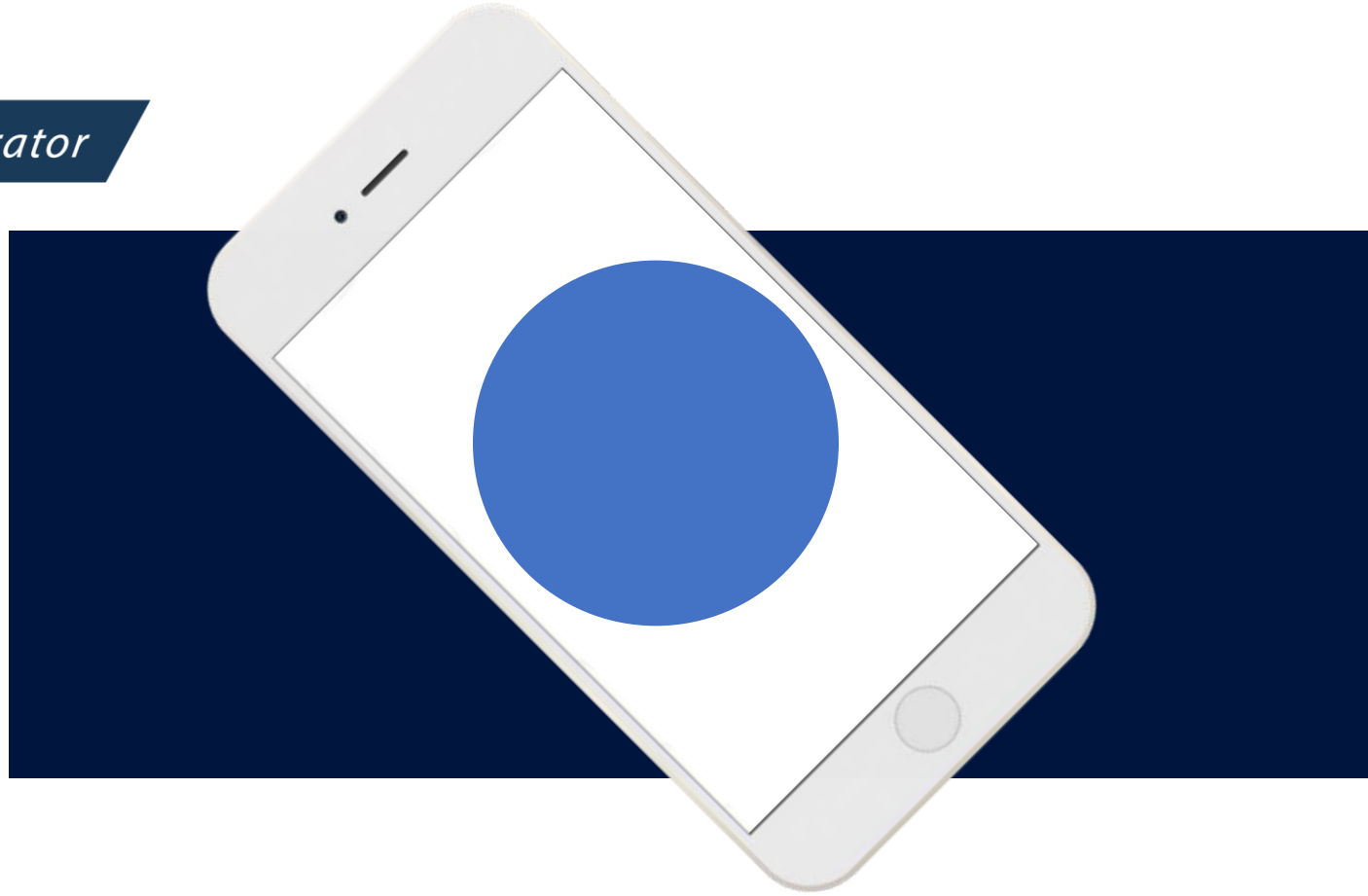
CMMC Assessment Guide – Level 2 v2.13	*dodcio.defense.gov/CMMC/Documentation*	**NIST SP 800-171 Rev 2**	*nvlpubs.nist.gov*
NIST SP 800-171A (Assessment Methods)	*nvlpubs.nist.gov*	**NIST SP 800-50 (Security Awareness)**	*csrc.nist.gov/publications*
NIST SP 800-181 NICE Framework	*niccs.cisa.gov*	**CISA Insider Threat Training**	*cisa.gov/insider-threat-mitigation*

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org



APEX ACCELERATORS

Cyber Thursday

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.

- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…More information and registrations at wispro.org/events

Federal Market Insights

Federal Market Insights [FMI] is an informal podcast designed to provide valuable information about the government marketplace for businesses interested in government contracting.

- **March 31** – CRADAs: Cooperative Research and Development Agreements
- **April 7** – Does Your Business Specialize in Critical Technology Areas?
- **April 14** – Unlocking DoD Opportunities for Nontraditional Contractors
- **April 21** – Is It Possible to Create Your Own Contract? Let's See What FAR 15.6 Says
- **April 28** –Seeking Innovative Research and Development (R&D) Ideas
- **May 5** – SAM Data Bank – Follow the Data to Identify Customers
- **May 12** – Navigating the Federal Laboratory Consortium: A Guide for Small Business Innovators

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

March 26 2026

This webinar is eligible for

1 CPE credit

To receive a certificate of completion, contact apexaccelerator@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MatthewF@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226