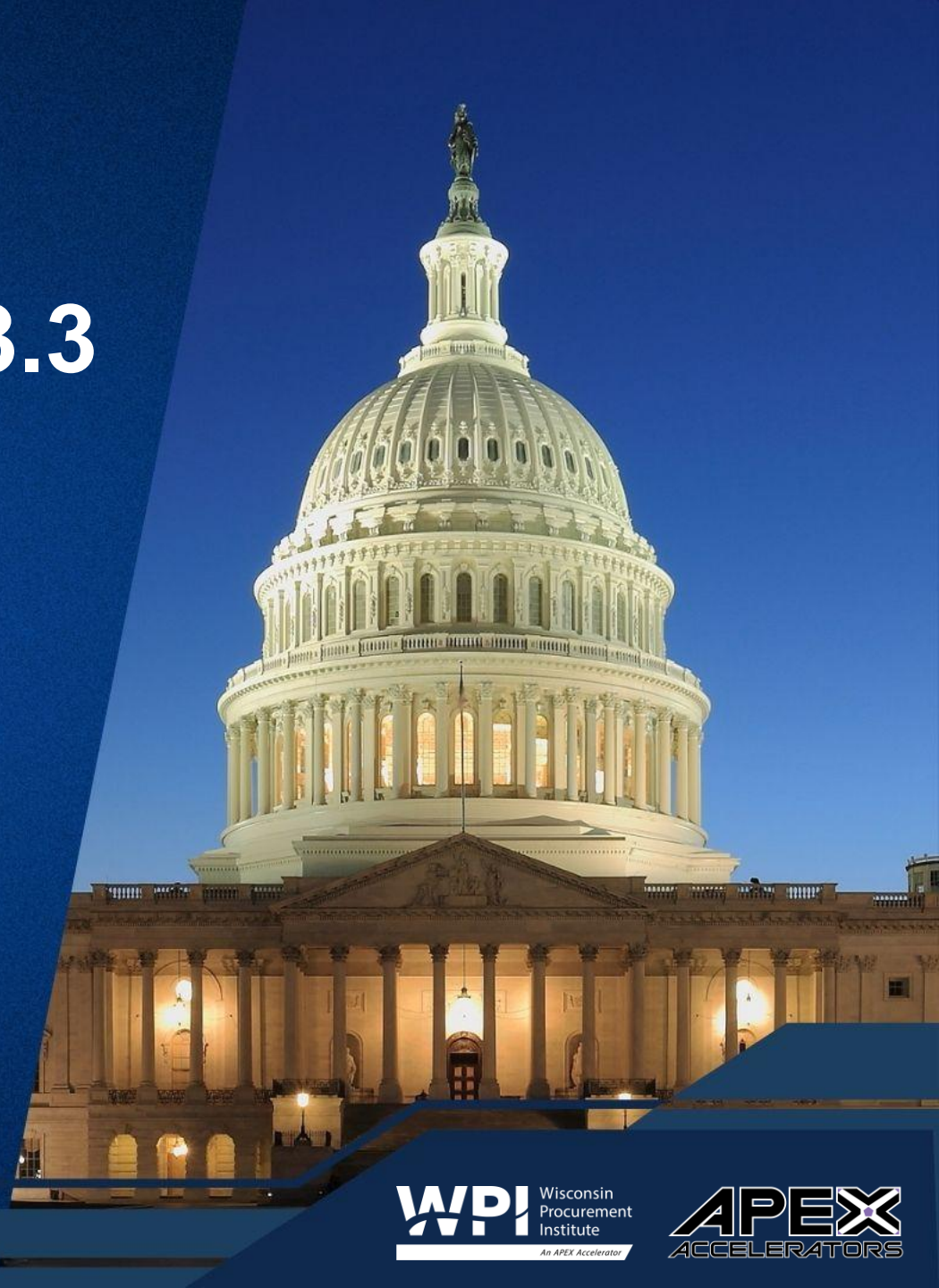
Cyber Thursday:

CMMC: Control Set Series: 3.3 Audit and Accountability

April 30 | 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute



WPI 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.

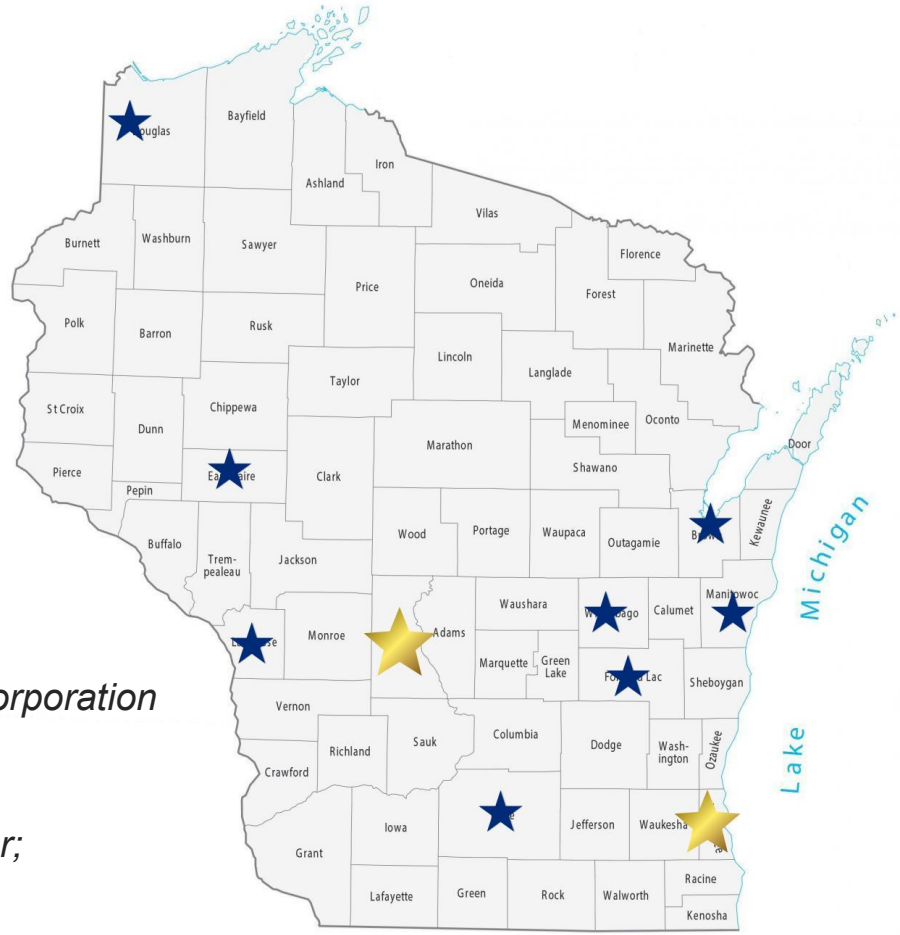
WPI provides services and training to all of Wisconsin's 72 counties

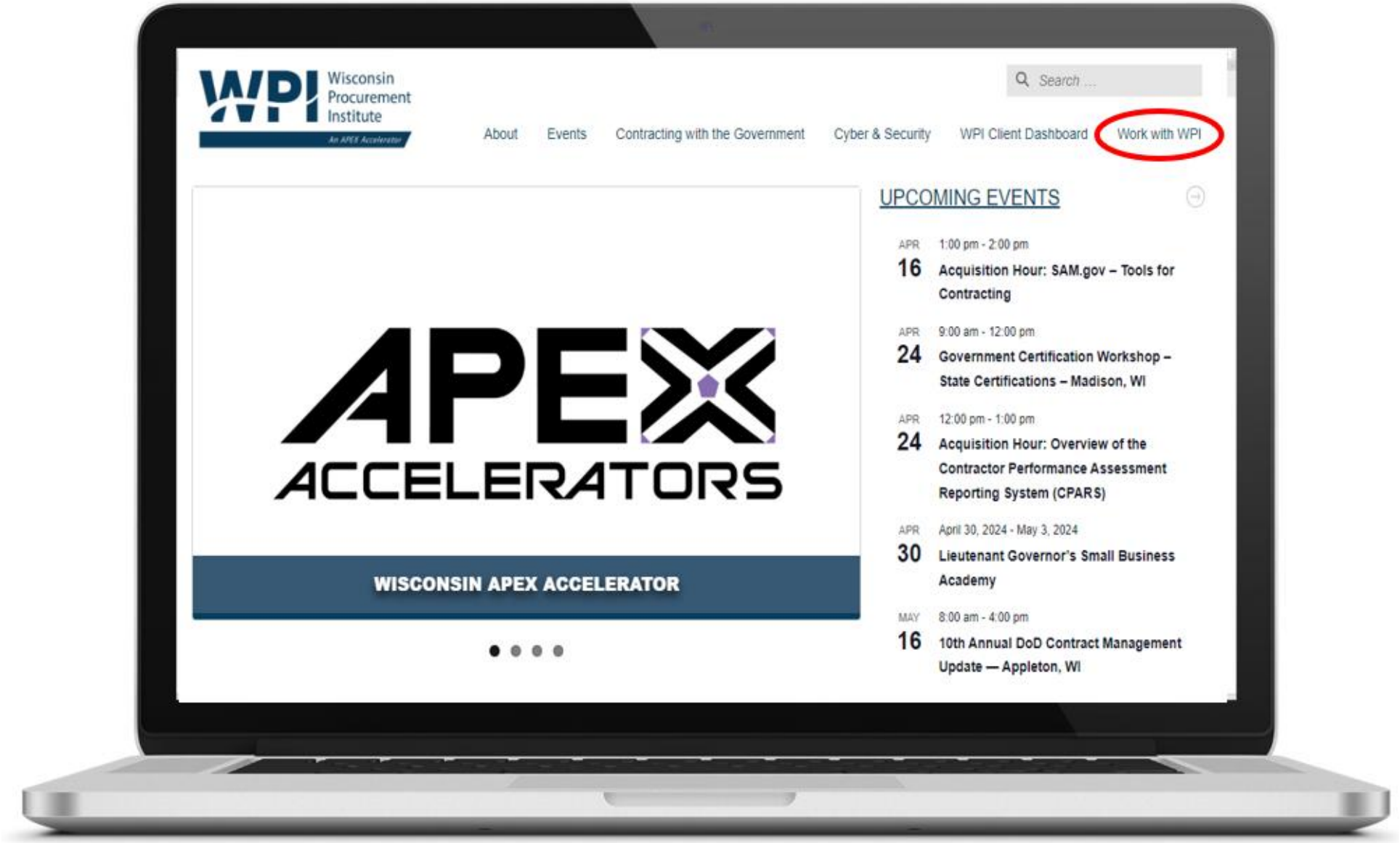
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting 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*

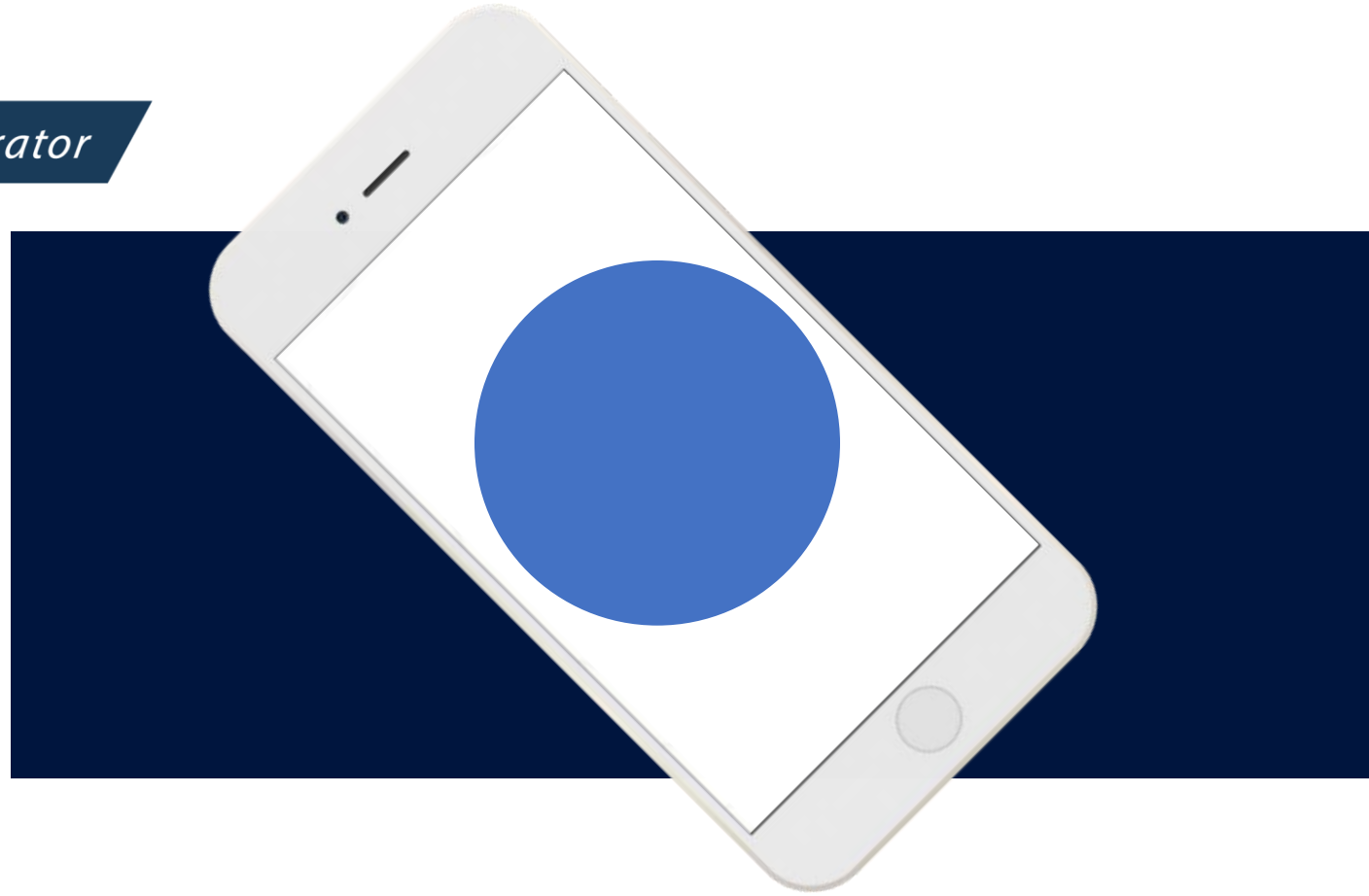



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR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

Audit and Accountability



Cyber Thursday – April 30th, 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

AU.L2-3.3.1 – SYSTEM AUDITING

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.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified;

[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined;

[c] audit records are created (generated);

[d] audit records, once created, contain the defined content;

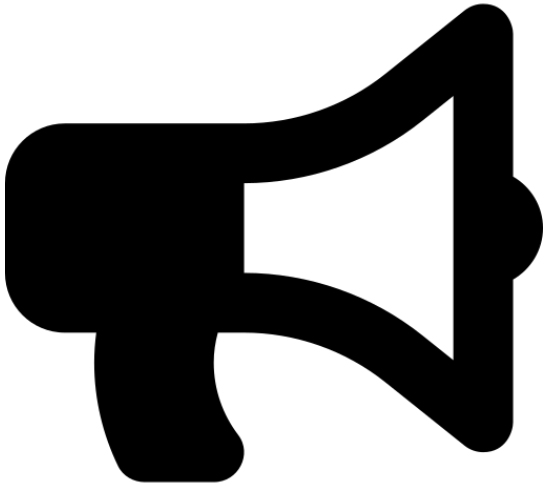
[e] retention requirements for audit records are defined; and

[f] audit records are retained as defined.

3.3.1	**SECURITY REQUIREMENT** 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.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.3.1[a] *audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.*
	3.3.1[b] *the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.*
	3.3.1[c] *audit records are created (generated).*
	3.3.1[d] *audit records, once created, contain the defined content.*
	3.3.1[e] *retention requirements for audit records are defined.*
	3.3.1[f] *audit records are retained as defined.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Audit and accountability policy; procedures addressing auditable events; system security plan; system design documentation; system configuration settings and associated documentation; procedures addressing control of audit records; procedures addressing audit record generation; system audit logs and records; system auditable events; system incident reports; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing system audit logging].

DOMAIN 3.3 · CONTROL AT.L2-3.3.1

System Auditing



If it isn't logged, it didn't happen – make every action traceable.

AU.L2-3.3.1 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

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.

ASSESSMENT OBJECTIVES — All six must be MET:

[a]	Audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.
[b]	The content of audit records needed to support monitoring, analysis, investigation, and reporting is defined.
[c]	Audit records are created (generated).
[d]	Audit records, once created, contain the defined content.
[e]	Retention requirements for audit records are defined.
[f]	Audit records are retained as defined.

AU.L2-3.3.1 – How to Implement: Building an Audit Logging Program

Step 1: Define What to Log

- Document the event types you must log: logons/logoffs, privileged actions, account changes, file access to CUI, configuration changes, security alerts
- Map each event type to the systems that produce it (servers, endpoints, firewalls, applications)
- Reference NIST SP 800-92 for guidance on event selection

Step 2: Define Record Content

- Each audit record must capture: what happened, when, where, source, outcome, and identity of the user/process
- Standardize timestamps to a consistent format (ISO 8601 recommended)
- Document the required fields in your SSP — assessors will check

Step 3: Generate & Centralize

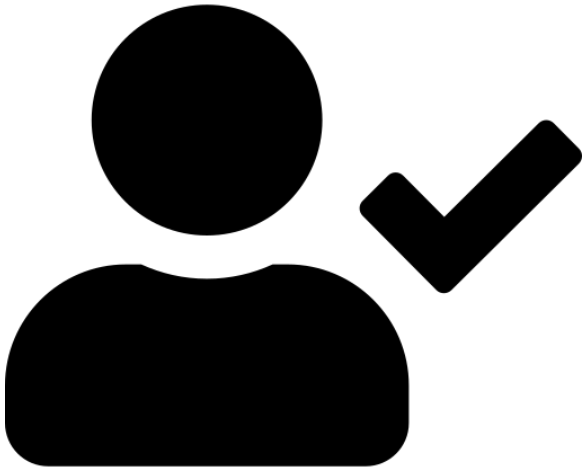
- Enable native logging on all in-scope systems (Windows Event Log, Linux auditd, etc.)
- Forward logs to a central repository or SIEM (Splunk, Elastic, Sentinel, Wazuh)
- Verify logs are flowing — gaps in coverage are a common audit finding

Step 4: Retain Per Policy

- Document a retention period in policy (CMMC requires you to define it; 1 year minimum is common practice)
- Implement archive storage for older logs — write-once or immutable preferred
- Test retrieval periodically to confirm records are readable

DOMAIN 3.3 · CONTROL AT.L2-3.3.2

User Accountability



Tie every action to a unique individual – no shared accounts, no anonymous events.

AU.L2-3.3.2 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

ASSESSMENT OBJECTIVES — All two must be MET:

[a]	The content of the audit records needed to support the ability to uniquely trace users to their actions is defined.
[b]	Audit records, once created, contain the defined content.

AU.L2-3.3.2 – Discussion Questions

DISCUSSION

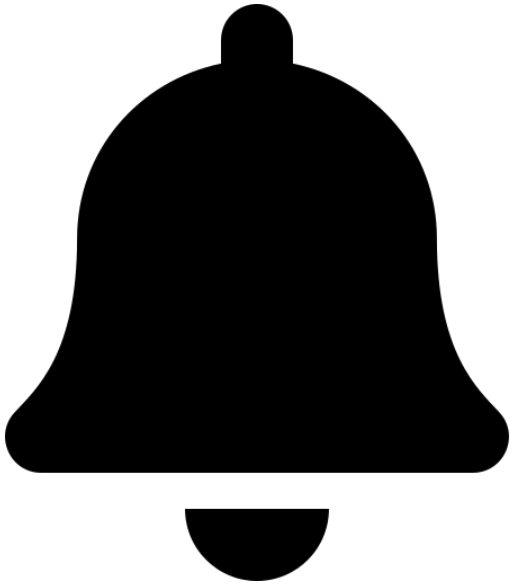
User accountability requires that every logged event identifies the unique individual who performed it. Shared accounts, generic service accounts without attribution, and anonymous actions break this control.

CONSIDER THE FOLLOWING:

1	Do all your in-scope systems require named individual logins, or are shared/generic accounts in use?
2	When privileged actions are taken (sudo, runas, admin escalation), can you trace them back to the specific human?
3	Do your service or system accounts have documented owners and a process to attribute their activity?

DOMAIN 3.3 · CONTROL AT.L2-3.3.3

Audit Logging Failure Alerts



Know within minutes when logging stops working – a silent SIEM is worse than no SIEM.

AU.L2-3.3.4 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Alert in the event of an audit logging process failure.

ASSESSMENT OBJECTIVES — All three must be MET:

[a]	Personnel or roles to be alerted in the event of an audit logging process failure are identified.
[b]	Types of audit logging process failures for which alert will be generated are defined.
[c]	Identified personnel or roles are alerted in the event of an audit logging process failure.

AU.L2-3.3.4 – Detecting and Alerting on Logging Failures

Step 1: Define Failure Types

- Storage exhaustion on log host or SIEM
- Log forwarder/agent stopped or unreachable
- Time gaps where no events arrived (heartbeat loss)
- Logging service crashed or disabled

Step 2: Identify Recipients

- Document the role(s) to be alerted in your SSP — typically SOC, IT operations, or security manager
- Provide both primary and secondary contacts to avoid single-point-of-failure
- Define after-hours escalation path

Step 3: Configure Detection

- Enable agent health monitoring in your SIEM or log management tool
- Set 'no events received in X minutes' alerts per critical source
- Monitor disk usage on log servers — alert at 70/85/95%

Step 4: Test & Document

- Periodically simulate a failure (stop a log agent in test) and verify alert fires
- Document the test results — assessors want evidence the alerting actually works
- Track mean-time-to-detection over time as a program metric

Foundations: Logging, Identity, and Time

THE BIG IDEA

Before any audit-and-accountability program can detect, attribute, or investigate, three foundational questions must already be answered: what gets recorded, who did it, and when did it really happen?

1

AU.L2-3.3.1

What Gets Logged

Define the events worth recording — logons, privileged actions, account changes, CUI access, configuration changes — and the content each record must capture. Without a defined event set, you can't prove coverage.

2

AU.L2-3.3.2

Who Did It

Every recorded action must trace back to a unique individual. Shared accounts, anonymous service identities, and unattributed privilege escalations break the chain of accountability that everything else depends on.

3

AU.L2-3.3.7

When It Happened

Timestamps from one host mean little unless every host shares the same authoritative clock. A consistent, synchronized time source is what allows logs from different systems to tell a coherent story.

BOTTOM LINE Get these three right and the rest of Domain 3.3 becomes evidence collection. Get any one wrong and your audit trail is unreliable on its face.

Readiness Checklist — AU.L2-3.3.1, 3.3.2, 3.3.7

AU.L2-3.3.1, 3.3.2, 3.3.7

Foundations: Logging, Identity, and Time

These three controls establish the baseline — without them, every other AU control is built on sand.

- [ ] 1 **Auditable event types documented in the SSP**
  Final, approved list covering logons, privileged actions, account changes, CUI access, config changes, and security alerts
- [ ] 2 **Required content fields defined per audit record**
  What, when, where, source, outcome, and identity — standardized format documented
- [ ] 3 **Logs generated on every in-scope system and centralized**
  SIEM or central repository; gaps in log forwarding coverage are a top finding
- [ ] 4 **Retention period defined and enforced**
  Policy specifies a duration (1+ year is common); archived logs retrievable on request
- [ ] 5 **Every in-scope system requires unique individual login**
  No shared accounts; service accounts have documented owners and attribution procedure
- [ ] 6 **Authoritative time source specified and configured**
  All in-scope hosts sync to it; drift monitoring in place; SSP names the source

✓ **Key evidence bundle: auditable events list (final) + retention policy + identity policy + time-sync configuration evidence**

Operations: Review, Alert, Correlate, Report

THE BIG IDEA

Foundation logging produces data; operations turn that data into a working detection and response capability. These four controls describe what happens between an event being recorded and someone actually doing something about it.

1

AU.L2-3.3.3

Stay Current

What you log today won't catch tomorrow's threats. Periodically review your event types — after major changes, after incidents, after threat intel updates — and adjust before gaps become findings.

2

AU.L2-3.3.4

Detect the Silence

A logging system that has stopped working is worse than none at all, because it gives false confidence. Failure alerting closes the gap by treating the absence of logs as itself a security event.

3

AU.L2-3.3.5

Connect the Dots

A real incident touches email, endpoints, identity, and network — not just one of them. Correlation is the discipline of stitching logs across sources so a single investigation tells one coherent story instead of four disconnected ones.

4

AU.L2-3.3.6

Make It Usable

Millions of raw log lines are useless to a human under time pressure. Reduction (search, filter, aggregate) and reporting (on-demand summaries) turn the haystack into something an analyst or auditor can actually work with.

BOTTOM LINE Operations is where logging stops being a checkbox and starts being a capability. Tools like a SIEM can be an answer — but the controls don't require one, they require the outcomes a tool would produce.

Readiness Checklist — AU.L2-3.3.3, 3.3.4, 3.3.5, 3.3.6

AU.L2-3.3.3, 3.3.4, 3.3.5, 3.3.6

Operations: Review, Alerting, Correlation, Reporting

These controls turn raw logs into a working detection-and-response capability.

- [ ] 1 **Logged-events review process documented**
  Trigger conditions for review (annually, post-incident, post-change) and outcomes recorded
- [ ] 2 **Logging-failure alerting configured and tested**
  Failure types defined, recipients identified; documented test confirms alert fires
- [ ] 3 **Cross-source correlation in place (SIEM rules or analyst playbook)**
  Multi-source patterns detectable; investigation workflow documented
- [ ] 4 **On-demand log search and reduction available to analysts**
  Query interface across all log sources; documented in SSP with screenshots
- [ ] 5 **On-demand report generation capability**
  Sample reports retained as evidence — by user, by time range, by event type
- [ ] 6 **Logging program reviewed and updated periodically**
  Records of past reviews and any resulting changes to the logged-events list

✓ **Key evidence bundle: review schedule + failure-alert config + correlation ruleset + sample reports + review meeting minutes**

Governance: Protection and Audit Management

THE BIG IDEA

Logs are forensic evidence — and like any evidence, they're worthless if they can be tampered with or if too many people can quietly turn them off. The last two controls protect the audit program from the very people who run it.

1

AU.L2-3.3.8

Protect the Trail

An attacker's first move after gaining a foothold is to delete or alter logs. Forward records off-host, restrict who can read or write them, and use tamper-evident or write-once storage so a compromised endpoint can't erase its own history.

2

AU.L2-3.3.9

Limit the Managers

Not every domain admin needs the ability to disable logging or change what's collected. A small, named subset of privileged users manages the audit program — separation of duties applied to the audit function itself.

BOTTOM LINE Governance is the assumption that someone — internal or external — will eventually try to undo your audit program. Build it so they can't, and so the attempt itself is logged.

Readiness Checklist — AU.L2-3.3.8, 3.3.9

AU.L2-3.3.8, 3.3.9

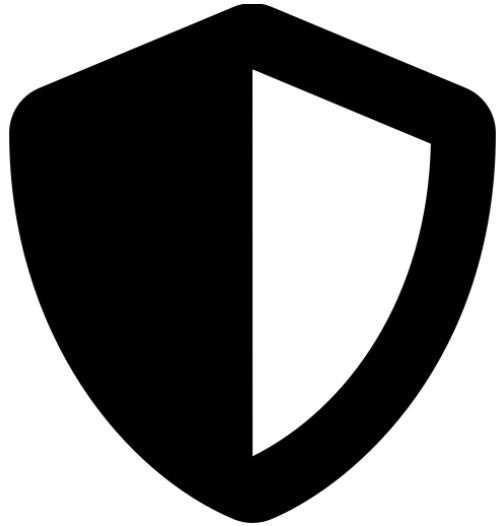
Governance: Protection and Audit Management

Logs are forensic evidence. These controls ensure they remain trustworthy and that not everyone can touch them.

- [ ] 1 **Access to audit information restricted and reviewed**
  Documented list of who can read logs; access reviewed at least annually
- [ ] 2 **Audit information protected from modification and deletion**
  Off-host forwarding to SIEM or WORM storage; tamper-evident controls in place
- [ ] 3 **Audit logging tools themselves access-controlled**
  SIEM admin console, agent configurations, and forwarders are restricted
- [ ] 4 **Changes to logging tools are themselves logged**
  A separate audit trail captures admin actions on the SIEM/log infrastructure
- [ ] 5 **Defined subset of privileged users for audit management**
  Named group documented in SSP; smaller than general sysadmin pool
- [ ] 6 **Domain/sysadmins prevented from disabling local logging**
  Group Policy or technical controls prevent unauthorized changes

✓ **Key evidence bundle: access list to logs + WORM/tamper-evidence config + audit-management group definition + change-log evidence**

Key Takeaways



- **Domain 3.3 is bigger than it looks — nine controls span what to log, who did it, when it happened, who watches, and who's allowed to manage the logs themselves**
- **3.3.1, 3.3.2, and 3.3.7 form the foundation: define your auditable events, attribute every action to an individual, and timestamp everything against an authoritative source**
- **3.3.3 through 3.3.6 are operational — review your event types, alert on logging failures, correlate across sources, and produce reports on demand**
- **3.3.8 and 3.3.9 are governance: protect the audit trail itself from tampering, and limit who can manage the logging program — including against your own admins**
- **Centralize logs off-host as early as possible — a SIEM (Splunk, Sentinel, Elastic, Wazuh) makes nearly every AU objective easier to evidence**

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 800-92 (Log Management Guide)
csrc.nist.gov/publications

NIST SP 800-53 Rev 5 (AU Family)
csrc.nist.gov/publications

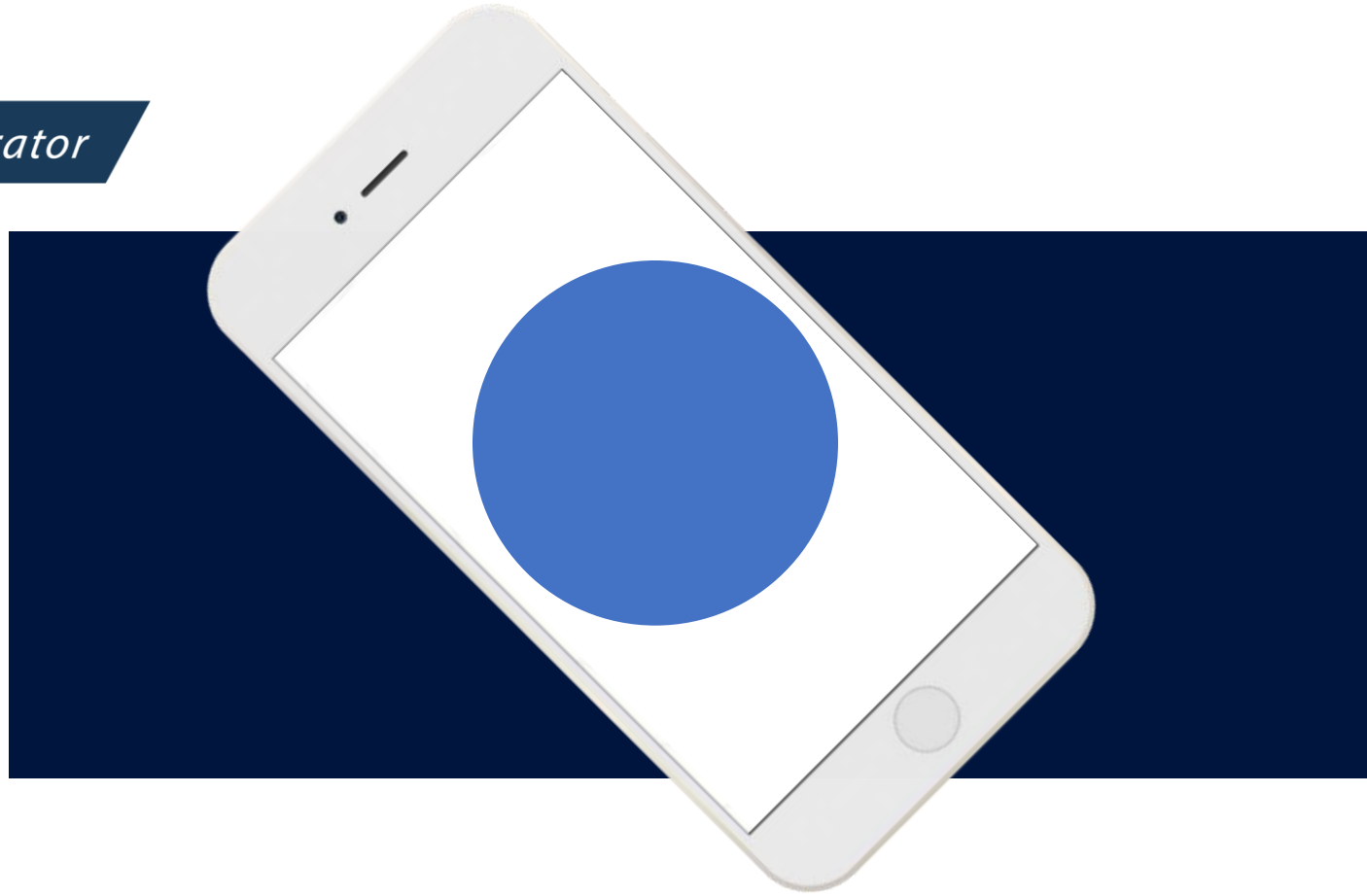
NTP / time.nist.gov
tf.nist.gov/tf-cgi/servers.cgi

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.

- **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.

- ~~**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

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **May 13** – CONTRACTING IN DISASTERS: Doing Business with Emergency Agencies
- **June 17** – Update on SBIR – STTR
- **June 3** – Things to Know When Contracting with the Federal Government

…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

April 30 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