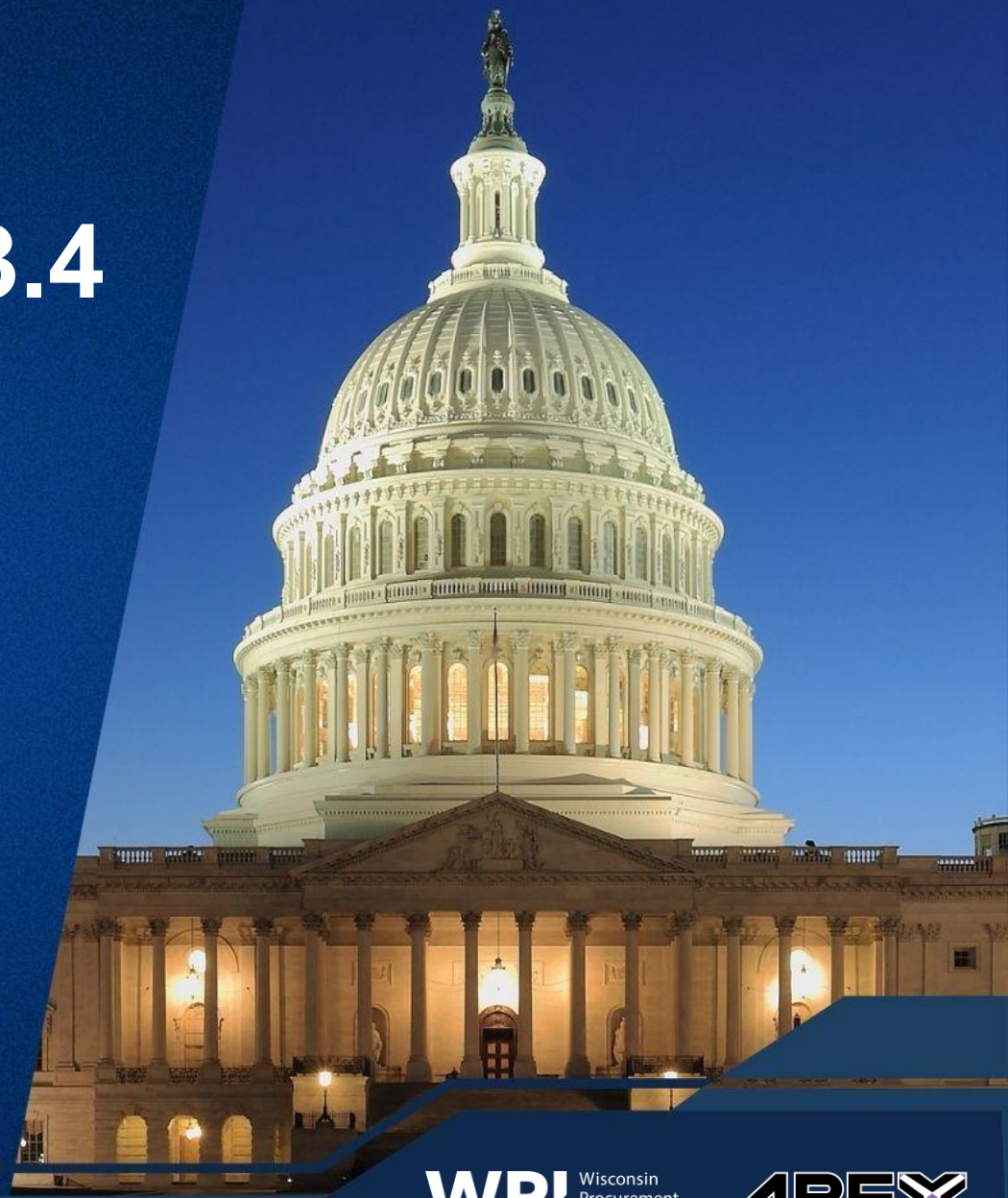
Cyber Thursday:

CMMC: Control Set Series: 3.4 Configuration Management

May 28| 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute



WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

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.

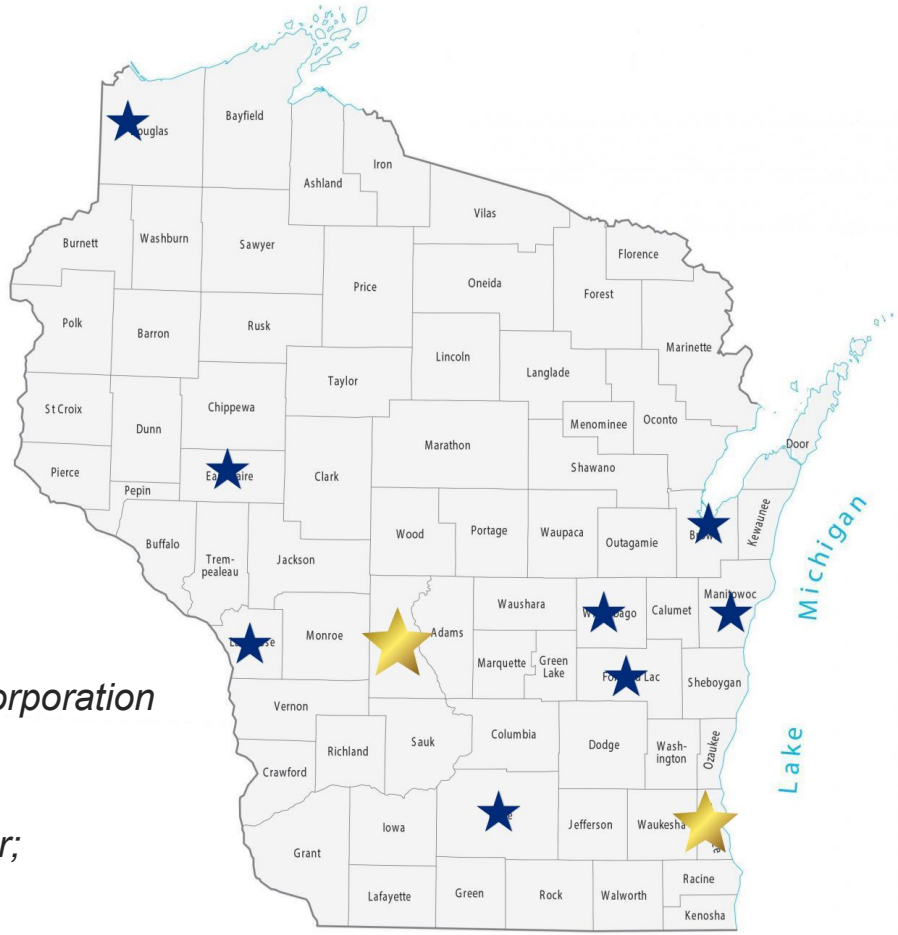
WPI provides services and training to all of Wisconsin's 72 counties

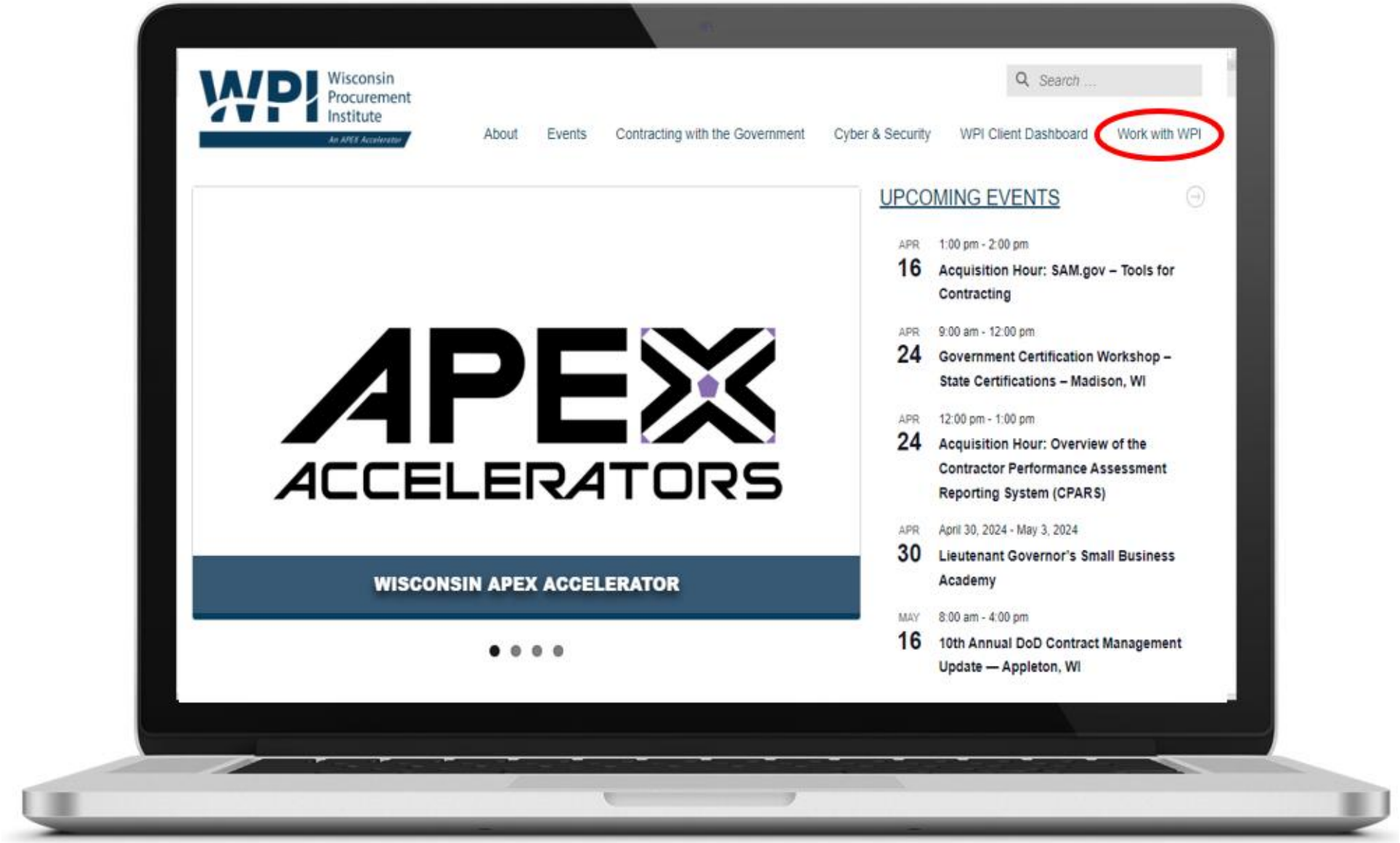
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting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

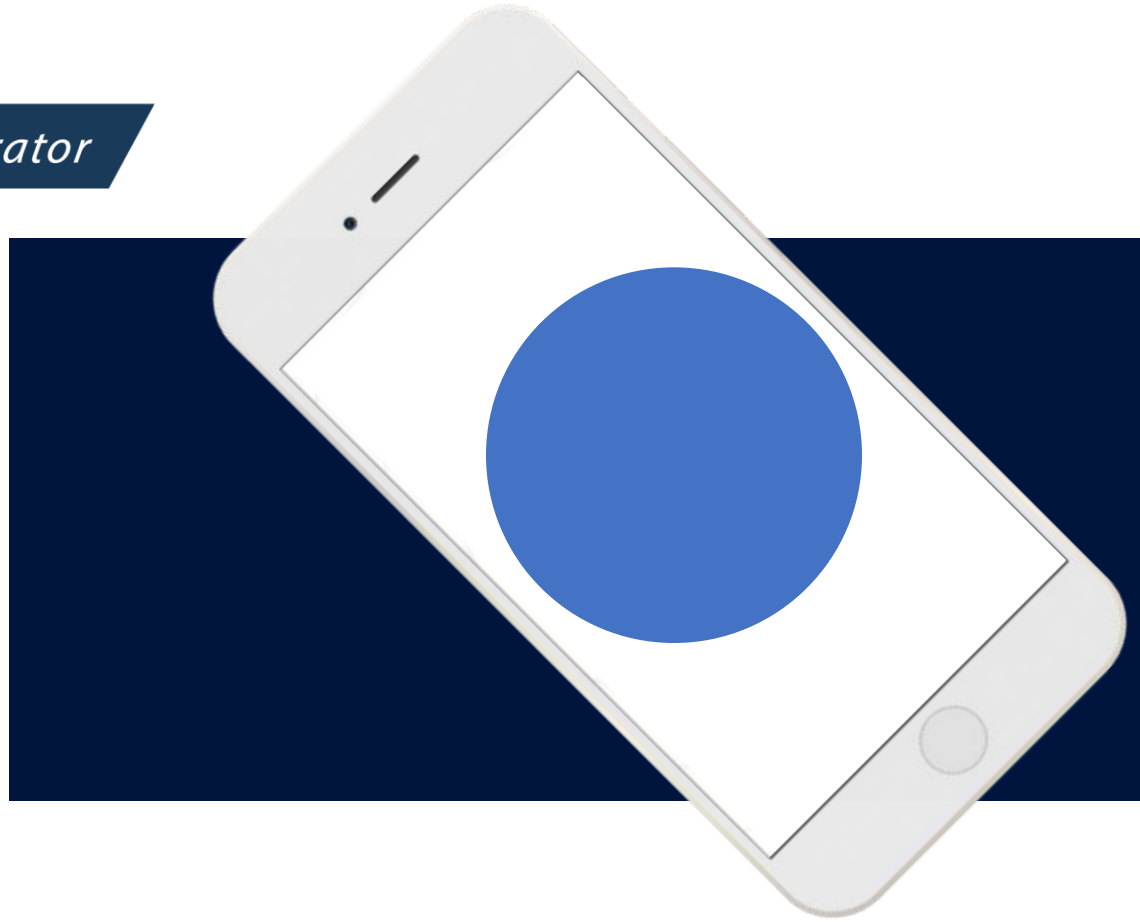



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR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

Configuration Management



Cyber Thursday – May 28th, 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

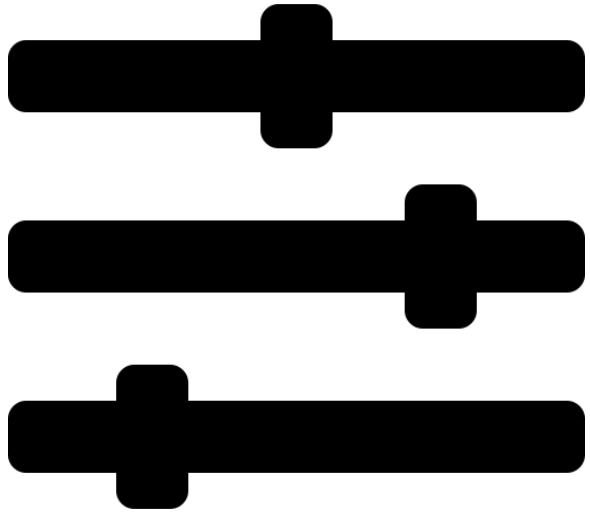
Level 2

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

DOMAIN 3.4 · CONFIGURATION MANAGEMENT

Configuration Management



You can't secure what you can't see — and you can't trust what you can't control.

Know What You Have

THE BIG IDEA

Every configuration management program starts with a documented, accurate picture of your systems. You cannot enforce a standard, detect a change, or investigate an incident if you don't first know what's supposed to be there.

1

BASELINE & INVENTORY

Document the Known-Good State

Establish and maintain baseline configurations — the approved, documented settings for your hardware, software, and firmware — plus an inventory of the systems those baselines apply to. The baseline is your reference point for everything else.

2

SECURITY SETTINGS

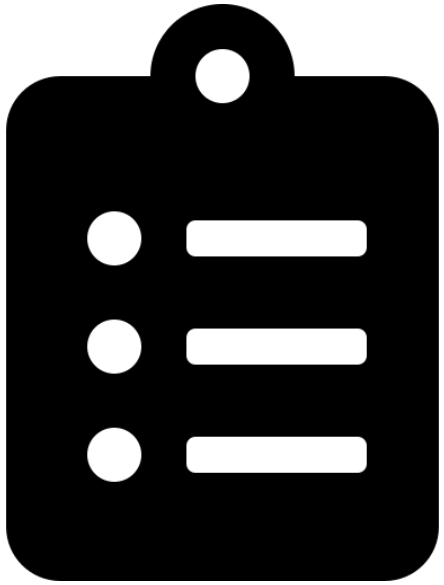
Define Secure Settings

Establish and enforce security configuration settings built into the products you use. Industry benchmarks (CIS, DISA STIGs, vendor hardening guides) give you a defensible, documented starting point instead of factory defaults.

BOTTOM LINE A baseline isn't a one-time document — it's the living reference that the rest of Domain 3.4 measures change against.

DOMAIN 3.4 · CONTROL CM.L2-3.4.1

Baseline Configurations & Inventories



Write down the known-good state — and keep a list of what it applies to.

CM.L2-3.4.1 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

ASSESSMENT OBJECTIVES — All six must be MET:

[a]	A baseline configuration is established.
[b]	The baseline configuration includes hardware, software, firmware, and documentation.
[c]	The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.
[d]	A system inventory is established.
[e]	The system inventory includes hardware, software, firmware, and documentation.
[f]	The inventory is maintained (reviewed and updated) throughout the system development life cycle.

CM.L2-3.4.1 – Building Baselines and Inventories

Step 1: Inventory Everything

- Catalog all hardware, software, firmware, and key documentation in scope
- Capture make/model, OS version, location, owner, and purpose
- Use automated discovery tools where possible — manual lists drift fast

Step 2: Define the Baseline

- Document the approved configuration for each system type
- Include installed software, settings, accounts, and patch level
- Reference CIS Benchmarks or vendor hardening guides as a starting point

Step 3: Store & Version It

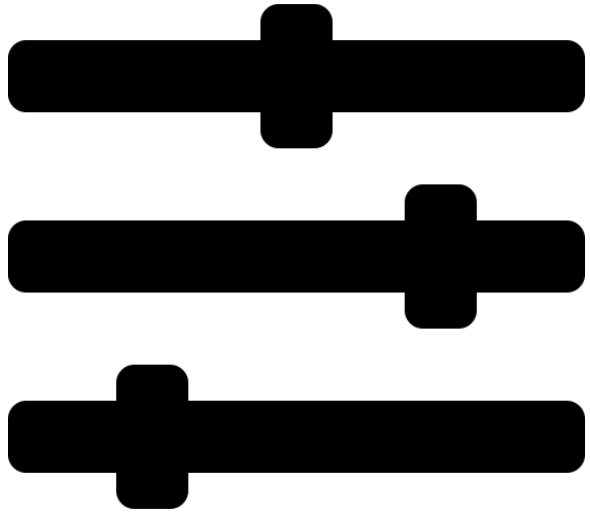
- Keep baselines under version control with dates and approvers
- Treat the baseline as a controlled document — not a one-off snapshot
- Make it retrievable; assessors will ask to see it

Step 4: Maintain Over Time

- Review and update baselines and inventory on a defined schedule
- Update when systems are added, retired, or significantly changed
- Tie maintenance to your change-control process (3.4.3)

DOMAIN 3.4 · CONTROL CM.L2-3.4.2

Security Configuration Settings



Don't ship factory defaults — define and enforce hardened settings.

CM.L2-3.4.2 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Establish and enforce security configuration settings for information technology products employed in organizational systems.

ASSESSMENT OBJECTIVES — All two must be MET:

[a]	Security configuration settings for information technology products employed in the system are established and included in the baseline configuration.
[b]	Security configuration settings for information technology products employed in the system are enforced.

CM.L2-3.4.2 – Establishing & Enforcing Secure Settings

Step 1: Pick a Standard

- Adopt recognized benchmarks: CIS Benchmarks, DISA STIGs, or vendor guides
- Choose the level appropriate to your risk and operational needs
- Document which standard applies to which product

Step 2: Bake Into Baseline

- Fold the chosen settings into your baseline configuration (3.4.1)
- Cover OS, browsers, productivity apps, network gear, and cloud tenants
- Record any deviations and the business reason for them

Step 3: Enforce Automatically

- Use Group Policy, Intune, MDM, or configuration tools to push settings
- Prevent users from changing security-relevant settings where possible
- Automated enforcement beats hoping people configure things correctly

Step 4: Monitor for Drift

- Scan periodically to confirm systems still match the secure settings
- Alert on drift and remediate; record the results as evidence
- Configuration scanners (e.g., compliance scanners) make this provable

Control How It Changes

THE BIG IDEA

Once you know your known-good state, the next job is making sure it only changes deliberately. Uncontrolled change is how secure systems quietly become insecure — these controls put a process, a review, and a gate around every change.

1

CHANGE CONTROL

Track & Approve Changes

Track, review, approve or disapprove, and log changes to your systems. A documented change-control process ensures every modification is intentional, recorded, and reversible — not a surprise discovered after something breaks.

2

IMPACT ANALYSIS

Analyze Before You Act

Analyze the security impact of a change before implementing it. A small change can open a large hole; impact analysis is the habit of asking "what does this affect?" before the change goes live, not after.

3

ACCESS RESTRICTION

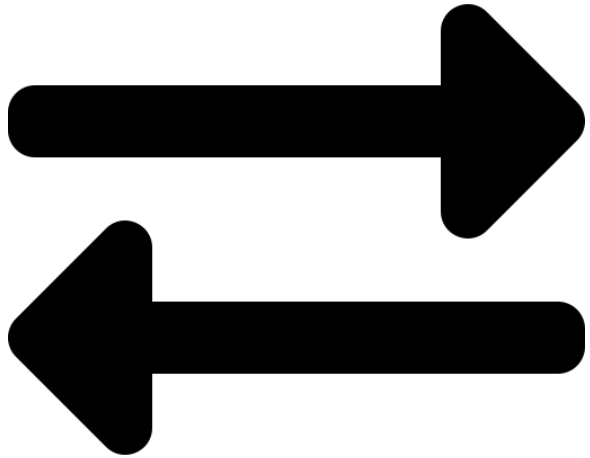
Limit Who Can Change

Define, document, approve, and enforce physical and logical access restrictions for making changes. Not everyone who can use a system should be able to reconfigure it — change rights are a privilege, granted deliberately.

BOTTOM LINE Change control is where configuration management becomes a discipline: every change is intentional, reviewed, authorized, and logged.

DOMAIN 3.4 · CONTROL CM.L2-3.4.3

Change Control & Tracking



Every change gets tracked, reviewed, approved or rejected, and logged.

CM.L2-3.4.3 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Track, review, approve or disapprove, and log changes to organizational systems.

ASSESSMENT OBJECTIVES — All four must be MET:

[a]	Changes to the system are tracked.
[b]	Changes to the system are reviewed.
[c]	Changes to the system are approved or disapproved.
[d]	Changes to the system are logged.

CM.L2-3.4.3 – Discussion Questions

DISCUSSION

Change control doesn't have to be heavyweight — even a small business can run a simple, documented process. The point is that changes are intentional and traceable, not made on a whim and forgotten.

CONSIDER THE FOLLOWING:

1	Do you have a defined process — even a simple ticket or form — for requesting and approving changes to in-scope systems?
2	Who reviews and approves changes, and is that authority documented? What happens with emergency changes?
3	Can you produce a log showing what changed, when, who approved it, and why — going back over time?

DOMAIN 3.4 · CONTROL CM.L2-3.4.4

Security Impact Analysis

Ask 'what could this break or expose?' before the change goes live.

CM.L2-3.4.4 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Analyze the security impact of changes prior to implementation.

ASSESSMENT OBJECTIVE — must be MET:

[a]	The security impact of changes to the system is analyzed prior to implementation.

CM.L2-3.4.4 – Discussion Questions

DISCUSSION

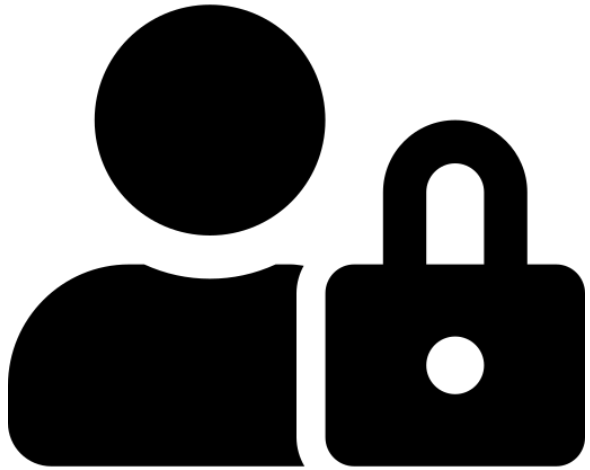
Security impact analysis is a step inside your change process: before a change is approved, someone considers how it affects the security posture of the system. It can be a checklist field on your change ticket — it doesn't require a separate program.

CONSIDER THE FOLLOWING:

1. When a change is proposed, does someone explicitly assess its security implications before it's approved?
2. Is the impact analysis recorded — for example, a required field or section in your change request?
3. For significant changes, do you test in a non-production environment before rolling out?

DOMAIN 3.4 · CONTROL CM.L2-3.4.5

Access Restrictions for Change



Reconfiguring a system is a privilege — grant it deliberately and enforce it.

CM.L2-3.4.6 – The Requirement & What Assessors Check

SECURITY REQUIREMENT

Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

ASSESSMENT OBJECTIVES — All two must be MET:

[a]	Essential system capabilities are defined based on the principle of least functionality.
[b]	The system is configured to provide only the defined essential capabilities.

Readiness Checklist — CM.L2-3.4.1, 3.4.2

CM.L2-3.4.1, 3.4.2

Know What You Have

You can't enforce or defend a configuration you haven't documented. These two controls establish your reference point.

- [ ] 1 **Baseline configuration documented and approved**
  Covers hardware, software, firmware, and documentation for each system type — final, not draft
- [ ] 2 **System inventory established and current**
  All in-scope assets cataloged with owner, location, version; reviewed and updated on a schedule
- [ ] 3 **Baseline maintained across the lifecycle**
  Updated when systems are added, changed, or retired — tied to your change-control process
- [ ] 4 **Security configuration settings defined**
  A recognized standard (CIS Benchmarks, DISA STIGs, vendor guides) chosen and folded into the baseline
- [ ] 5 **Secure settings enforced, not just written**
  Pushed via Group Policy / Intune / MDM; users can't change security-relevant settings
- [ ] 6 **Configuration drift detected and remediated**
  Periodic scans confirm systems still match the baseline; results retained as evidence

✓ **Key evidence bundle: baseline configuration document + asset inventory + chosen hardening standard + drift-scan results**

Readiness Checklist — CM.L2-3.4.3, 3.4.4, 3.4.5

CM.L2-3.4.3, 3.4.4, 3.4.5

Control How It Changes

Uncontrolled change is how secure systems quietly become insecure. These three controls put a gate around every change.

- [ ] 1 **Documented change-control process exists**
  Even a simple ticket/form — changes are requested, reviewed, approved or disapproved, and logged
- [ ] 2 **Change log maintained over time**
  Shows what changed, when, who approved it, and why; retrievable for the assessment period
- [ ] 3 **Security impact analysis built into the process**
  Security implications of a change are assessed and recorded before approval
- [ ] 4 **Significant changes tested before production**
  Non-production testing for higher-risk changes where feasible
- [ ] 5 **Change access restrictions defined and approved**
  Both physical and logical — documented list of who may make configuration changes
- [ ] 6 **Change restrictions actually enforced**
  Privileged rights limited technically; physical access to equipment controlled; enforcement demonstrable

✓ **Key evidence bundle: change-management policy + change log/tickets + impact-analysis records + approved change-access list**

Readiness Checklist — CM.L2-3.4.6, 3.4.7, 3.4.8, 3.4.9

CM.L2-3.4.6, 3.4.7, 3.4.8, 3.4.9

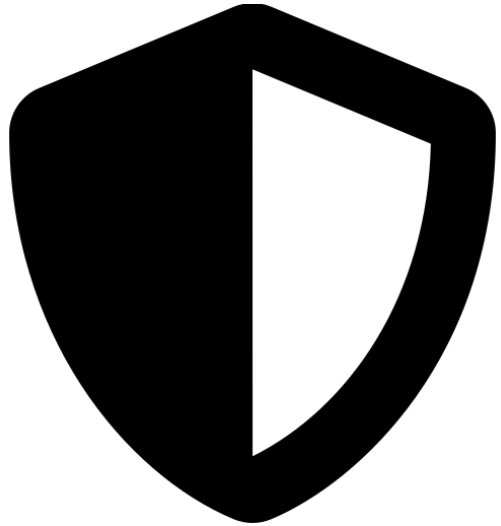
Reduce Your Attack Surface

The most secure component is the one that isn't running. These four controls turn off, lock down, and account for everything nonessential.

- [ ] 1 **Essential capabilities defined; rest removed**
  Least functionality — systems configured to provide only what they need; unused features uninstalled/disabled
- [ ] 2 **Nonessential ports, protocols, services closed**
  Defined and restricted/disabled at host and network; legacy insecure protocols turned off; verified by scan
- [ ] 3 **Execution policy chosen and documented**
  Allowlisting (preferred) or denylisting decided, with the list of allowed/denied software maintained
- [ ] 4 **Execution policy technically enforced**
  AppLocker, WDAC, or endpoint tooling enforces the policy — not just a written statement
- [ ] 5 **User software-installation policy established**
  Clear rules on what users may install; admin rights removed from standard users; approval path defined
- [ ] 6 **User-installed software monitored**
  Regular software inventory compared against policy; unauthorized installs flagged and reviewed

✓ **Key evidence bundle: least-functionality definitions + port/service scans + execution-policy config + user-install policy + software inventory**

Key Takeaways



- Domain 3.4 tells one story in three parts: know what you have, control how it changes, and reduce your attack surface
- Everything starts with the baseline and inventory — you can't enforce, detect, or investigate against a state you never documented
- Change control is the discipline at the center: every change tracked, reviewed, authorized, impact-analyzed, and logged, by a limited set of people
- Attack-surface reduction is the highest-leverage payoff — least functionality, closed ports/services, execution allowlisting, and governed user installs
- Most of these controls are about documentation plus enforcement: assessors want to see the policy AND proof it's actually applied (scans, logs, configs)

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 800-128 (Config Management)
csrc.nist.gov/publications

CIS Benchmarks
cisecurity.org/cis-benchmarks

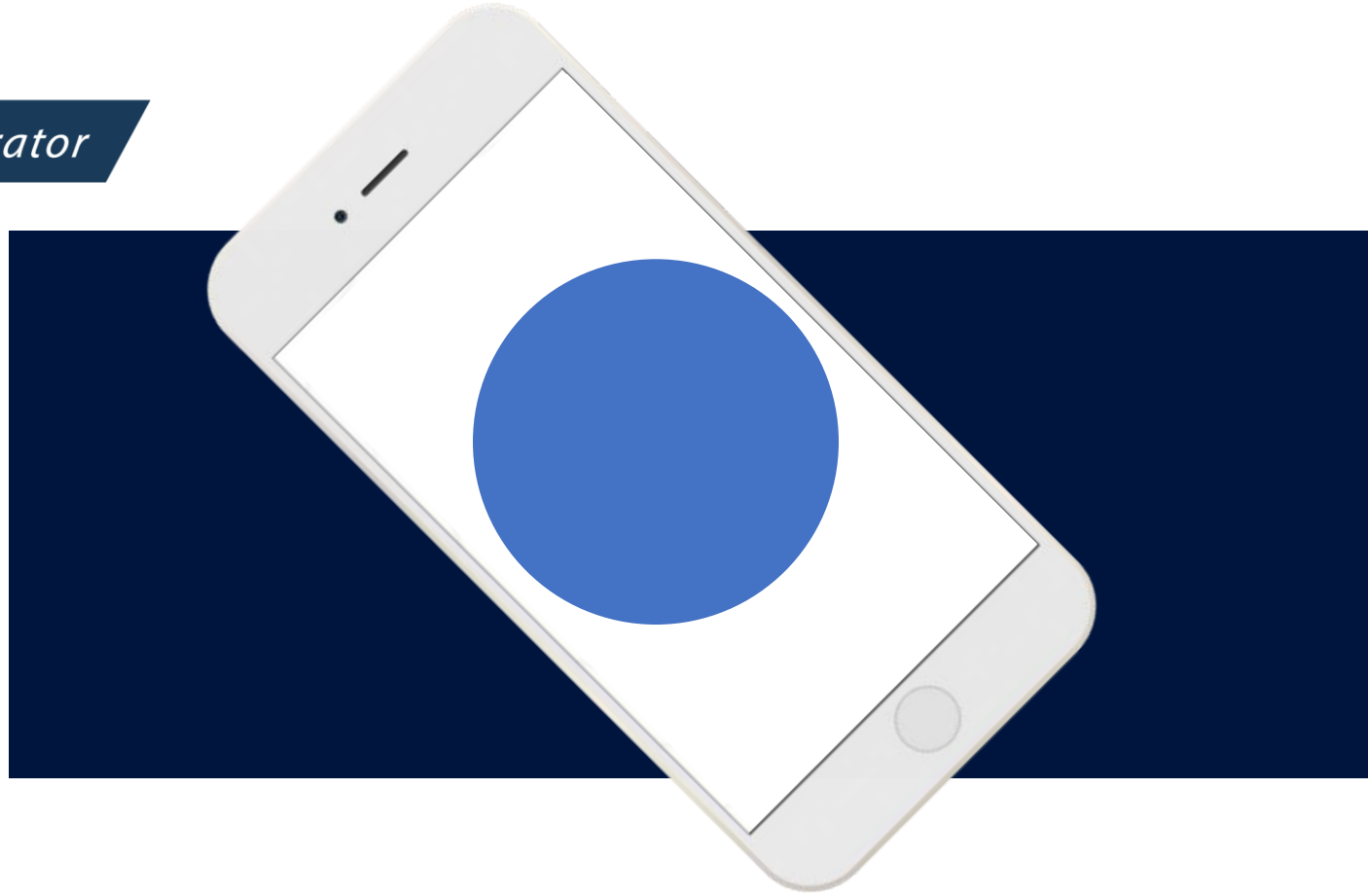
DISA STIGs
public.cyber.mil/stigs

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.

- ~~May 28 – CMMC: Control Set Series: 3.4 Configuration Management~~
- June 25 – Cybersecurity Requirements for Non-Department of War Contractors and Suppliers
- July 16 – A Guide to Strong Supporting Documentation
- August 27 – Determining Your Real CMMC Compliance Responsibilities

…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.

- ~~May 12 – Navigating the Federal Laboratory Consortium: A Guide for Small Business Innovators~~
- ~~May 19 – Federal Innovation Sites Every Inventor Should Know~~
- ~~May 26 – IP, Data Rights, and Federal Awards: What Every Company Should Know~~
- June 2 – Unsolicited Proposals & NSF Project Pitches: Paths Beyond SBIR Topics
- June 9 – Beyond the Capabilities Statement

…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.

- June 3 – Things to Know When Contracting with the Federal Government
- June 17 – Update on SBIR – STTR

…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

May 28 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