CMMC Level 2 (NIST SP 800-171)

Gap Assessment Report
Demonstration Project

Prepared by Palladian Cyber

This is a demonstration project created to showcase my methodology for CMMC Level 2 / NIST 800-171 gap assessments and remediation planning. It is not a real client engagement and does not represent a certified assessment.

Executive Summary

Palladian Cyber conducted a demonstration CMMC Level 2 / NIST SP 800-171 gap assessment to evaluate the readiness of a fictional small U.S.-based defense subcontractor that handles Controlled Unclassified Information (CUI). The assessment focused on identifying gaps between current practices and CMMC Level 2 requirements, prioritizing remediation actions appropriate for a small organization, and preparing the organization for a future formal assessment.

While basic security hygiene is present, multiple controls lack sufficient formalization, documentation, and retained evidence to meet CMMC Level 2 expectations.

Summary of Findings

1. Access Control (AC): Partially Implemented
2. Identification & Authentication (IA): Partially Implemented
3. Audit & Accountability (AU): Implemented but Fragile
4. Configuration Management (CM): Implemented but Fragile
5. Incident Response (IR): Not Implemented
6. Risk Assessment (RA): Partially Implemented

Assessment Scope, Boundary, and Assumptions

This assessment assumes a fictional U.S.-based small defense subcontractor with approximately 18 employees and a limited, informal IT/security function. The organization operates a mixed macOS and Linux environment, maintains a small on-prem Linux server, and uses limited cloud services to support operations involving CUI.

In-scope systems include macOS and Linux endpoints used by staff who access CUI, the on-prem Linux server supporting internal services, cloud services used to store, process, or transmit CUI, user accounts with access to CUI, and policies and procedures related to handling CUI.
Out-of-scope systems include personal devices not used for company work, marketing and public-facing systems, and financial/HR systems that do not handle CUI.

This assessment is aligned to CMMC Level 2 and NIST SP 800-171 Rev. 2 and focuses on practical, evidence-based evaluation rather than theoretical or enterprise-grade implementations.

Access Control (AC) — Partially Implemented

Control Reference

NIST SP 800-171: 3.1.6
CMMC Level 2 Domain: Access Control (AC)

Control Requirement (Plain English)

The organization must limit system access to authorized users and ensure that access privileges are granted based on job responsibilities and least privilege principles. Access must be reviewed and removed when no longer required.

Current State (Assumed)

Palladian Cyber’s assessment determined that the organization has implemented basic access controls across macOS and Linux systems. Individual user accounts are used for daily operations, and access to systems containing CUI is generally restricted to staff with a business need.

However, access provisioning and deprovisioning are handled informally. There is no documented process for approving access, reviewing user privileges, or ensuring timely removal of access when roles change or employment ends. Access reviews are performed on an ad hoc basis and rely primarily on institutional knowledge rather than defined procedures.

Gap Identified

- No documented procedure for granting, modifying, or revoking access
- No defined cadence for reviewing user access rights
- No centralized record demonstrating approval or validation of access decisions
- Inability to consistently demonstrate least-privilege enforcement to an assessor

Risk / Impact

Without a formal access management process, former employees or contractors may retain access to systems containing CUI, users may accumulate excessive privileges over time, and unauthorized access may go undetected. During a CMMC Level 2 assessment, the absence of documented access control procedures and review evidence could result in a finding of non-compliance.

Recommended Remediation

- Define access criteria based on role and job function
- Require documented approval for new or modified access
- Establish a formal access revocation process for role changes and terminations
- Conduct periodic access reviews (e.g., quarterly) for systems handling CUI

Small-Team Implementation Notes

- Maintain a simple access register listing users, systems, and access levels
- Assign access approval responsibility to a designated role
- Retain evidence of completed quarterly access reviews
- Leverage existing OS-level access controls with documented procedures

Identification & Authentication (IA) — Partially Implemented

Control Reference

NIST SP 800-171: 3.5.3
CMMC Level 2 Domain: Identification & Authentication (IA)

Control Requirement (Plain English)

The organization must use multifactor authentication (MFA) for network access to privileged accounts and for access to systems that process, store, or transmit Controlled Unclassified Information (CUI).

Current State (Assumed)

Unique user accounts are used and basic password requirements are enforced. MFA is enabled for some externally accessible services and select cloud platforms.

However, MFA enforcement is inconsistent. Internal systems handling CUI do not uniformly require MFA, privileged access paths are not clearly differentiated, and no written standard defines MFA scope or requirements.

Gap Identified

- MFA is not uniformly enforced for all access to CUI
- Privileged and administrative access paths are not clearly defined
- No documented MFA standard or enforcement policy exists
- Limited evidence demonstrating consistent MFA application

Risk / Impact

Inconsistent MFA enforcement increases the risk that compromised credentials could be used to access systems handling CUI. During a CMMC assessment, partial MFA implementation without documentation may result in a non-compliance finding.

Recommended Remediation

- Define systems and access types requiring MFA
- Document approved MFA mechanisms and configurations
- Validate MFA enforcement across all in-scope systems
- Retain evidence demonstrating consistent MFA implementation

Small-Team Implementation Notes

- Leverage built-in MFA capabilities of existing platforms
- Standardize MFA expectations across services
- Document MFA requirements in policy
- Periodically validate MFA during access reviews

Audit & Accountability (AU) — Implemented but Fragile

Control Reference

NIST SP 800-171: 3.3.1
CMMC Level 2 Domain: Audit & Accountability (AU)

Control Requirement (Plain English)

The organization must generate, retain, and review audit logs to detect, investigate, and analyze unauthorized or inappropriate activity on systems that handle CUI.

Current State (Assumed)

Audit logging is enabled on systems handling CUI, and logs are retained and accessible for troubleshooting.

However, log review is informal and reactive, with no documented procedures, cadence, or retained evidence of routine review.

Gap Identified

- No documented log review procedures
- No defined review cadence or scope
- No retained evidence of routine log review
- Dependence on individual knowledge rather than institutional process

Risk / Impact

Suspicious activity may go undetected, and assessors may determine the control is not institutionalized due to lack of documentation and evidence.

Recommended Remediation

- Document which logs must be reviewed
- Define review frequency and scope
- Assign log review responsibility
- Retain evidence of completed reviews

Small-Team Implementation Notes

- Use native OS and application logs
- Create a simple log review checklist
- Assign primary and backup reviewers
- Record reviews in existing documentation or ticketing tools

Configuration Management (CM) — Implemented but Fragile

Control Reference

NIST SP 800-171: 3.4.1
CMMC Level 2 Domain: Configuration Management (CM)

Control Requirement (Plain English)

The organization must establish and maintain baseline configurations and control changes to systems that handle CUI.

Current State (Assumed)

Systems are configured using secure defaults and standardized practices, but baselines are undocumented and change management relies on informal communication.

Gap Identified

- No documented configuration baselines for CUI systems
- No defined change approval or tracking process
- Limited retained evidence demonstrating configuration control

Risk / Impact

Configuration drift and undocumented changes may occur, and the organization may be unable to demonstrate effective configuration control during an assessment.

Recommended Remediation

- Document baseline configurations for in-scope systems
- Establish a lightweight change approval process
- Track significant configuration changes
- Periodically validate systems against baselines

Small-Team Implementation Notes

- Maintain simple baseline configuration documents
- Track changes using tickets or version-controlled files
- Perform baseline reviews after major changes or quarterly

Incident Response (IR) — Not Implemented

Control Reference

NIST SP 800-171: 3.6.1
CMMC Level 2 Domain: Incident Response (IR)

Control Requirement (Plain English)

The organization must establish an incident response capability that includes preparation, detection, analysis, containment, recovery, and post-incident activities for security incidents involving systems that handle CUI.

Current State (Assumed)

The organization does not have a formal incident response plan or documented procedures. Incidents are handled informally without defined roles or escalation paths.

Gap Identified

- No documented incident response plan
- No defined incident response roles or responsibilities
- No formal incident identification or escalation process
- No post-incident review or lessons-learned process

Risk / Impact

Security incidents involving CUI may not be detected or escalated promptly, response actions may be inconsistent, and assessment evidence cannot be produced.

Recommended Remediation

- Define what constitutes a security incident
- Establish incident response roles and responsibilities
- Document detection, analysis, containment, and recovery steps
- Define escalation and notification requirements
- Require documentation and post-incident review

Small-Team Implementation Notes

- Create a concise incident response plan (2–4 pages)
- Assign primary and backup incident response leads
- Track incidents using existing ticketing or documentation tools
- Conduct an annual tabletop exercise

Risk Assessment (RA) — Partially Implemented

Control Reference

NIST SP 800-171: 3.11.1
CMMC Level 2 Domain: Risk Assessment (RA)

Control Requirement (Plain English)

The organization must periodically assess risk to organizational operations, assets, and individuals resulting from the operation of systems that handle CUI.

Current State (Assumed)

Leadership and technical staff informally consider risk during planning and remediation prioritization.

However, there is no documented risk assessment methodology, no defined review cadence, and no centralized record of identified risks or mitigation decisions.

Gap Identified

- No documented risk assessment process
- No defined schedule for risk review
- No centralized risk register or tracking mechanism
- Risk discussions are not consistently documented or retained

Risk / Impact

Risk management may be viewed as ad hoc during an assessment, and high-risk issues may not be consistently prioritized or tracked.

Recommended Remediation

- Define a risk identification and evaluation methodology
- Create and maintain a centralized risk register
- Establish a periodic risk review cadence
- Use risk findings to inform remediation planning

Small-Team Implementation Notes

- Maintain a simple risk register document or spreadsheet
- Assign ownership for periodic review
- Focus on high-impact risks related to CUI