PalladianCyber

CMMC Level 2 (NIST SP 800-171)

Implementation Plan & Remediation Roadmap
Demonstration Report

Prepared by Palladian Cyber

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

Implementation Plan Overview

This implementation plan builds on the findings identified in the CMMC Level 2 (NIST SP 800-171) Gap Assessment Demonstration Report. The purpose of this document is to outline prioritized remediation actions that are realistic, achievable, and appropriate for a small organization handling Controlled Unclassified Information (CUI).

The plan emphasizes feasibility, documentation, and evidence generation rather than enterprise-scale tooling.

Guiding Principles

- Focus on closing assessment gaps with minimal operational disruption
- Prioritize documentation and repeatability
- Leverage existing tools and open-source solutions where possible
- Align remediation activities with staffing and budget constraints
- Generate and retain evidence artifacts that map directly to control requirements

Phased Remediation Approach

Phase 1: Immediate Actions (0–30 Days)

- Formalize access control procedures (approval, modification, revocation) and assign accountability
- Define MFA requirements and enforce MFA for all access paths to CUI systems (including privileged access)
- Draft and approve an incident response plan; define roles and escalation paths
- Create an initial risk register and capture known risks tied to CUI handling

Phase 2: Short-Term Actions (30–90 Days)

- Execute the first quarterly access review and retain evidence of completion
- Document audit log review procedures and begin routine reviews with retained checklists/records
- Document configuration baselines for in-scope systems and establish change tracking
- Conduct an incident response tabletop exercise and retain exercise notes and corrective actions

Phase 3: Ongoing Activities (90+ Days)

- Refine policies and procedures based on findings, incidents, and tabletop outcomes
- Validate consistency of control implementation across all in-scope systems
- Maintain documentation and evidence for assessment readiness (continuous compliance rhythm)
- Prepare for engagement with a CCP/CCA or C3PAO, including evidence packaging and interview readiness

Control-to-Remediation Mapping

This table provides traceability between identified gaps and remediation actions. It also highlights the evidence artifacts that would be expected during a formal CMMC Level 2 assessment.

Control / Domain	Gap Summary	Remediation Action	Expected Evidence
AC 3.1.6 Access Control	Access provisioning/deprovisioning and periodic reviews are informal; insufficient retained evidence.	Implement documented access approval, revocation, and quarterly access reviews for all CUI systems.	Access control procedure; access register; quarterly review log; termination checklist evidence.
IA 3.5.3 Identification & Authentication	MFA enforcement is inconsistent for systems and access paths involving CUI.	Define MFA standard; enforce MFA for all CUI access (including privileged access) and validate coverage.	MFA policy/standard; configuration screenshots; system list showing MFA enabled; review evidence.
AU 3.3.1 Audit & Accountability	Logs exist but routine reviews are undocumented; limited repeatability/evidence.	Document log review process; execute routine reviews on defined cadence; retain results.	Log review SOP; checklist; dated review records; sample investigated events/tickets.
CM 3.4.1 Configuration Management	Baseline configurations are not documented; change tracking is informal.	Document baselines for in-scope systems; implement lightweight change approval/tracking.	Baseline docs; approved change records; config snapshots; validation notes.
IR 3.6.1 Incident Response	No formal incident response plan, roles, escalation path, or testing.	Create IR plan; assign roles; establish reporting/escalation; conduct annual tabletop exercise.	Incident response plan; contact/escalation list; incident ticket template; tabletop exercise notes.
RA 3.11.1 Risk Assessment	Risk assessment methodology and cadence are undocumented; no maintained risk register.	Establish risk assessment process; maintain centralized risk register; review on defined cadence.	Risk assessment procedure; risk register; meeting notes showing periodic review and decisions.