nerdio

NERDIO RESOURCE

CMMC compliance guide for IT professionals

CMMC has 3 levels of maturity:

Level 1 (Foundational)
Basic cyber hygiene practices protecting federal contract information (FCI).

Level 2 (Advanced)
Compliance with NIST SP 800-171 practices for safeguarding CUI.

Level 3 (Expert)
Advanced controls mapped to NIST SP 800-172 for protection against advanced persistent threats (APTs).

Organizations must meet the required CMMC level to bid on or renew DoD contracts, making adherence non-negotiable.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a compliance framework established by the Department of Defense (DoD) to safeguard controlled unclassified information (CUI) across its supply chain. Organizations must meet specific cybersecurity standards and obtain third-party certification to continue working on DoD contracts.

Key technical steps to achieve CMMC compliance

The Cybersecurity Maturity Model Certification (CMMC) is a compliance framework

1. Conduct a gap analysis

- Map your existing security controls to the 110 practices outlined in NIST SP 800-171 for Level 2 or NIST SP 800-172 for Level 3.
- Identify gaps in access control, incident response, and audit logging.

2. Build a System Security Plan (SSP)

- Develop a detailed SSP documenting your organization's current cybersecurity infrastructure, configurations, and processes.
- Ensure the SSP addresses the assessment objectives for each CMMC domain (e.g., access control, configuration management, and risk assessment).
- Identify gaps in access control, incident response, and audit logging.

Pro tips for IT Professionals

Streamline compliance scope

Leverage Microsoft Azure's certified infrastructure to create secure enclaves for CUI, reducing assessment scope and complexity.protecting federal contract information (FCI).

Integrate policy automation

Tools such as Nerdio Manager help enforce compliance by automating the deployment of CIS and CMMC-aligned security policies.

Leverage centralized reporting

Nerdio Manager provides a single-pane-of-glass view for tracking compliance metrics, reducing time spent on manual audits.

Prepare for real-time threats

Use advanced endpoint detection and response (EDR) tools in conjunction with Nerdio to protect against APTs, as required for Level 3 compliance.

3. Implement mandatory practices

- Map your existing security controls to the 110 practices outlined in NIST SP 800-171 for Level 2 or NIST SP 800-172 for Level 3.
- Identify gaps in access control, incident response, and audit logging.
- Deploy continuous monitoring solutions to identify and mitigate vulnerabilities proactively.

4. Prepare for third-party assessments

- Gather evidence of compliance, such as audit logs, security configurations, and employee training records.
- Use tools that centralize and automate audit preparation to streamline assessor reviews.

CMMC compliance checklist for IT professionals

- [ ] Conduct a gap analysis using NIST SP 800-171 and CMMC Assessment Guides.
- [ ] Develop a comprehensive SSP and plan of action & milestones (POA&M) for identified gaps.
- [ ] Implement access controls, encryption protocols, and endpoint protection to secure systems.
- [ ] Establish an incident response plan (IRP) aligned with NIST guidelines.
- [ ] Maintain audit logs and system monitoring in accordance with CMMC Level 2 or 3 requirements.
- [ ] Train employees on role-specific cybersecurity protocols and insider threat awareness.
- [ ] Schedule a third-party assessment with a CMMC C3PAO.

Why CMMC compliance is essential

Maintain DoD contract eligibility	Advanced controls mapped to NIST SP 800-172 for protection against advanced persistent threats (APTs).
Reduce cyber risks	Implementing CMMC practices significantly mitigates risks of data breaches and insider threats.
Build competitive advantage	Demonstrating compliance builds trust with clients and positions your organization as a leader in cybersecurity maturity.

Learn how Nerdio Manager simplifies and cost optimizes the deployment and management of native Microsoft cloud technologies.

About Nerdio

Nerdio is a premier software solution provider, supporting organizations of all sizes looking to deploy, manage, and cost-optimize native Microsoft technologies. We partner with Managed Service Providers (MSPs) and enterprise organizations all over the world to add value on top of their existing Microsoft investments like Azure Virtual Desktop, Windows 365, and Microsoft Intune.

nerdio

WEB www.getnerdio.com
EMAIL hello@getnerdio.com

PO42425000