

CMMC 2.0 Self-Assessment Template

Use this template to assess your organization's compliance with CMMC 2.0 Level 2 requirements (110 NIST SP 800-171 controls). Document your implementation status and identify gaps.

ASSESSMENT INFORMATION

Organization Name: _____

Assessment Date: _____

Assessor Name: _____

Target CMMC Level: & Level 1 (17 controls) & Level 2 (110 controls) & Level 3 (110+ controls)

ACCESS CONTROL (AC) - 22 Requirements

- AC.L1-3.1.1 - Limit system access to authorized users
 - AC.L1-3.1.2 - Limit system access to authorized functions
 - AC.L2-3.1.3 - Control CUI flow in accordance with approved authorizations
 - AC.L2-3.1.4 - Separate duties of individuals to reduce risk
 - AC.L2-3.1.5 - Employ least privilege principle
 - AC.L2-3.1.6 - Use non-privileged accounts for non-security functions
 - AC.L2-3.1.7 - Prevent non-privileged users from executing privileged functions
- ... and 15 additional AC controls (see full NIST 800-171)

AWARENESS AND TRAINING (AT) - 3 Requirements

- AT.L2-3.2.1 - Security awareness training for all users
- AT.L2-3.2.2 - Role-based security training for personnel with security responsibilities
- AT.L2-3.2.3 - Insider threat awareness training

AUDIT AND ACCOUNTABILITY (AU) - 9 Requirements

- AU.L2-3.3.1 - Create and retain system audit logs
- AU.L2-3.3.2 - Ensure actions can be traced to individual users
- AU.L2-3.3.3 - Review and update audit events
- AU.L2-3.3.4 - Alert on audit logging process failure

CMMC 2.0 Self-Assessment Template

COMPLIANCE SCORING SUMMARY

Domain	Total Controls	Implemented	Score %
Access Control (AC)	22	—	—
Awareness & Training (AT)	3	—	—
Audit & Accountability (AU)	9	—	—
Configuration Management (CM)	9	—	—
Identification & Authentication (IA)	11	—	—
Incident Response (IR)	3	—	—
Maintenance (MA)	6	—	—
Media Protection (MP)	9	—	—
Personnel Security (PS)	2	—	—
Physical Protection (PE)	6	—	—
Risk Assessment (RA)	3	—	—
Security Assessment (CA)	4	—	—
System & Comm Protection (SC)	16	—	—
System & Info Integrity (SI)	7	—	—
TOTAL	110	—	—

NEXT STEPS

1. Complete assessment of all 110 controls against your environment
2. Document evidence for each implemented control
3. Create POA&M for controls not yet implemented
4. Engage C3PAO for formal assessment (Level 2)
5. Submit results to SPRS (Supplier Performance Risk System)

Need CMMC compliance assistance?

Forge Cyber Defense specializes in DIB compliance
info@forgecyberdefense.com | www.forgecyberdefense.com

www.forgecyberdefense.com

© 2025 Forge Cyber Defense. All rights reserved.