CMMC Level 2 Knowledge Base

Overview

CMMC (Cybersecurity Maturity Model Certification) Level 2 serves as a transitional step between the foundational security requirements in Level 1 and the advanced requirements of Level 3. It is aligned with the 110 security controls in NIST SP 800-171 and focuses on the protection of Controlled Unclassified Information (CUI).

Objectives of CMMC Level 2

- Protect Controlled Unclassified Information (CUI)
- Implement 110 security practices from NIST SP 800-171
- Establish documented policies and procedures
- Demonstrate process maturity at the 'documented' level

Key Features

- All Level 1 practices are included
- Adds 93 additional practices for a total of 110
- Practices span across 14 domains
- Requires documentation of practices and policies

Core Domains and Example Practices

1. Access Control (AC)

- Limit system access to authorized users
- Control internal system access
- Control remote system access

2. Audit and Accountability (AU)

- Create and retain audit logs

- Review and analyze logs for indications of suspicious activity

3. Configuration Management (CM)

- Establish and maintain baseline configurations

- Enforce security configuration settings

4. Identification and Authentication (IA)

- Use multi-factor authentication

- Identify and authenticate organizational users and devices

5. Incident Response (IR)

- Establish an incident response capability

- Track, document, and report incidents

6. Maintenance (MA)

- Perform maintenance on organizational systems

- Control and monitor maintenance tools

7. Media Protection (MP)

- Protect CUI on digital and non-digital media

- Sanitize media before disposal or reuse

8. Personnel Security (PS)

- Screen individuals before authorizing access to systems

- Ensure personnel termination procedures

9. Physical Protection (PE)

- Limit physical access to systems and facilities

10. Risk Assessment (RA)

- Conduct regular risk assessments

- Address discovered vulnerabilities

11. Security Assessment (CA)

- Develop and implement system security plans

- Monitor security controls regularly

12. System and Communications Protection (SC)

- Protect CUI in transit and at rest

- Deny network traffic by default

13. System and Information Integrity (SI)

- Identify, report, and correct system flaws

- Protect against malware and other threats

14. Awareness and Training (AT)

- Provide cybersecurity training for users

- Ensure users are aware of security risks

Assessment Requirements

- CMMC Level 2 assessments must be conducted by a certified C3PAO

- Contractors handling CUI must undergo triennial third-party assessments

- Requires evidence of implementation and documentation of policies

Compliance Tips

- Maintain updated and detailed security documentation
- Regularly review access permissions and configurations
- Conduct simulated phishing exercises
- Stay current with vulnerability scanning and patching
- Prepare for assessment by performing internal audits

Conclusion

CMMC Level 2 introduces a significant increase in cybersecurity rigor compared to Level 1. It represents a shift from basic cyber hygiene to more structured, documented, and repeatable processes aimed at protecting Controlled Unclassified Information (CUI). Achieving and maintaining Level 2 compliance demonstrates a serious commitment to cybersecurity and is essential for organizations handling CUI.