Cybersecurity Maturity Model Certification Checklist

Level 1: Basic Cyber Hygiene

Access Control (AC)

- ☐ Limit system access to authorized users.
- ☐ Use strong passwords and implement password policies.
- ☐ Regularly review and update user access permissions.
- ☐ Implement multi-factor authentication (MFA) for remote access.

Identification and Authentication (IA)

- ☐ Establish user identities before granting access.
- ☐ Use unique usernames and secure authentication mechanisms.
- ☐ Employ multi-factor authentication for all privileged accounts.

System and Communications Protection (SC)

- ☐ Install and regularly update antivirus and anti-malware software.
- ☐ Implement firewalls to protect networks from unauthorized access.
- ☐ Encrypt sensitive data during transmission (e.g., SSL/TLS).

Level 3: Good Cyber Hygiene

Configuration Management (CM)

- ☐ Establish and maintain a baseline configuration for systems.
- ☐ Regularly update and patch software and hardware components.
- ☐ Document and track changes to configurations.

Incident Response (IR)

- ☐ Develop an incident response plan and team.
- ☐ Regularly test and update the incident response plan.
- ☐ Monitor systems for signs of unauthorized access or breaches.
- ☐ Train employees on recognizing and reporting security incidents.

Security Training and Awareness (ST)

- ☐ Provide cybersecurity training to all employees.
- ☐ Regularly communicate security best practices and threats.

Level 5: Advanced Cyber Hygiene

Audit and Accountability (AU)

- ☐ Implement automated audit log collection and review.
- ☐ Retain audit logs for an appropriate period.
- ☐ Regularly analyze audit logs for signs of unauthorized activity.

System and Information Integrity (SI)

- ☐ Employ mechanisms to detect and prevent unauthorized changes.
- ☐ Regularly monitor systems for signs of compromise.
- ☐ Implement integrity checks for critical software and data.

Advanced Threat Protection (ATP)

- ☐ Deploy advanced threat detection tools.
- ☐ Regularly conduct penetration testing and vulnerability assessments.

Important Reminder:

This checklist is designed to help you get started, but keep in mind that CMMC requirements and guidelines can change over time. It's vital to refer to the official CMMC resources for accurate information.

Before you download or use this checklist:

1. Check for Updates: Ensure that the checklist aligns with the latest CMMC standards.
2. Tailor to Your Needs: Adapt it to match your organization's specific requirements.

Remember, cybersecurity is a dynamic field. Stay informed and stay secure by staying current with the official CMMC guidelines and industry best practices.

EDAFIO

Empowering IT. Powered by people.