CMMC Kill Chain

version 2023.1

Here is corresponding text and reasoning for the CMMC Kill Chain :

Phase 1: Define CUI. This should be self-explanatory and is based on your contract(s) to define what CUI is for your specific business case.

Phase 2: Establish Scoping. This has four subcomponent steps to define the scope of the CMMC assessment boundary:
(1) Create a Data Flow Diagram (DFD) that shows how CUI flows from the DoD all the way down to subcontractors;
(2) Create a detailed asset inventory for all systems, applications and services for both in-scope and out-of-scope assets;
(3) Create a detailed network diagram that includes where CUI is stored, transmitted and/or processed; and
(4) Inventory Third-Party Service Providers (TSP) to determine TSP access to CUI and/or in-scope systems, applications and/or services.

Phase 3: Documentation. This has two subcomponent steps to document the CUI environment:
(1) Start populating the System Security Plan (SSP); and
(2) Create a Plan of Action & Milestone (POA&M) to track and remediate deficiencies.

Phase 4: Secure Architecture. This involves implementing a network architecture that ensures it is built on secure engineering principles and enclaves to protect sensitive information (e.g., FCI/CUI). POA&M deficiencies & document procedures.

Phase 5: Resource Prioritization. This has six subcomponent steps to plan, identify gaps and prioritize resources:
(1) Define applicable statutory, regulatory and contractual obligations (including DFARS, FAR, NIST 800-171 and CMMC);
(2) Perform a gap assessment from applicable statutory, regulatory and contractual obligations;
(3) Develop & implement policies and standards to address applicable statutory, regulatory and contractual obligations;
(4) Identify the necessary People, Processes & Technology (PPT) that are necessary and appropriately sized;
(5) Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet compliance obligations; and
(6) Prioritize objectives from the resource plan for PPT requirements. POA&M any deficiencies from this phase.

Phase 6: Procedures / Rules of Behavior. This has two subcomponent steps:
(1) Develop & implement procedures to implement policies & standards; and
(2) Define processes to securely handle CUI. POA&M any deficiencies from this phase.

Phase 7: Risk Management. Develop & implement a Risk Management Program (RMP) to identify, assess and remediate risk. POA&M deficiencies & document procedures.

Phase 8: Change Management. Develop & implement change control processes, including a Change Control Board (CCB). POA&M deficiencies & document procedures.

Phase 9: Incident Response Operations. Develop & implement incident response capabilities to detect, respond and recover from incidents. POA&M deficiencies & document procedures.

Phase 10: Situational Awareness. Develop & implement situational awareness capabilities through log collection and analysis (e.g., SIEM). POA&M deficiencies & document procedures.

Phase 11: Baseline Security Configurations. Identify, build & implement secure baseline configurations (e.g., hardening standards) for all technology platforms. POA&M deficiencies & document procedures.

Phase 12: Centralized Controls Management. Build & implement Group Policy Objects (GPOs) for Microsoft Active Directory (AD). POA&M deficiencies & document procedures.

Phase 13: Identity & Access Management. Develop & implement Identity & Access Management (IAM) to address "least privilege" and Role-Based Access Control (RBAC). POA&M deficiencies & document procedures.

Phase 14: Maintenance. Develop & implement proactive maintenance practices. POA&M deficiencies & document procedures.

Phase 15: Vulnerability Management. Develop & implement Attack Surface Management (ASM) practices. POA&M deficiencies & document procedures.

Phase 16: Asset Management. Develop & implement technology asset management practices. POA&M deficiencies & document procedures.

Phase 17: Personnel Security. Work with Human Resources (HR) to ensure personnel security requirements are integrated into HR operations. POA&M deficiencies & document procedures.

Phase 18: Network Security. Develop & implement network security practices. POA&M deficiencies & document procedures.

Phase 19: Business Continuity. Develop & implement business continuity capabilities. POA&M deficiencies & document procedures.

Phase 20: Encryption. Develop & implement cryptographic key management and data encryption capabilities. POA&M deficiencies & document procedures.

Phase 21: Physical Security. Develop & implement physical security practices. POA&M deficiencies & document procedures.

Phase 22: Security Awareness Training. Build and maintain a security-minded workforce through training & awareness. POA&M deficiencies & document procedures.

Phase 23: Internal Audit. Build and maintain an "internal audit" or Information Assurance (IA) capability to govern controls. POA&M deficiencies & document procedures.

Guidance on some of the reasoning used in developing this model:

1. You can't legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management/risk threshold. Risk management is the key building block. (e.g., evidence of due diligence).

2. Once you have solid risk management practices, change control is the second most important phase to address, since that is needed to legitimately alter other practices and you need to be able to document your changes and track open issues in a POA&M (e.g., evidence of due care).

3. From there, the assumption is that you will discover issues so incident response capability needs to exist (e.g., DFARS incident reporting requirements).

4. Event logging/SIEM is next and needs to exist before secure configurations, since logs need to get sent somewhere. You need to have this logging infrastructure in place before you get into secure configurations.

5. Secure configurations and centralized management (e.g., GPOs) almost go hand-in-hand, but before you can centrally manage configurations, they need to be defined and standardized.

6. Next, identity and access management needs to be locked down to ensure aspects of least privilege and RBAC are implemented. The reason IAM comes after secure configurations is due to troubleshooting - if you have "gold standard" secure builds to work from, it is easier to then assign permissions/RBAC that will work with those builds. The alternative is your new configs break your IAM/RBAC, which is bad. Avoid that.

7. You realistically can't do vulnerability management without first having solid maintenance capabilities, so maintenance needs to be formalized with change control integrations. Maintenance needs to be tied into change management, which has a risk management component to it.

8. The concept of vulnerability management is broad and is best summed up by the term "attack surface management" where you are doing what you can to minimize the ways an adversary can attack. This relies on maintenance practices and change management being in place and operating.

9. From there, the remaining phases are relatively subjective - it really is. However, the "internal audit" function realistically needs to come last where control validation testing assesses how well controls are implemented. This can help serve as a pre-audit function.