CMMC Kill Chain

A Phase-Based Model To Prioritize CMMC 2.0 Pre-Assessment Activities

Version 2024.1

Table of Contents

EXECUTIVE SUMMARY

The concept of creating a "CMMC Kill Chain" was to create a proof of concept for an efficient way to plan out a roadmap to successfully pass a Cybersecurity Maturity Model Certification (**CMMC**) assessment. The end result is a viable approach for anyone to use in order to create a prioritized project plan for CMMC pre-assessment activities.

Why "CMMC Kill Chain" you ask? The concept of a kill chain is simply that it is easier to stop and prevent further damage if those malicious activities are discovered earlier, rather than later. When you look at CMMC's zero tolerance for deficiencies, if you have a single deficiency in a process or practice, you will fail your CMMC assessment. Given that reality with CMMC, the intention of using the CMMC Kill Chain is that if you apply a prioritized, phased approach towards CMMC-related pre-assessment activities, it is possible to avoid rework and cascading failures by addressing dependencies earlier in the process. The bottom line is this model breaks down CMMC into 23 major steps, which can then be translated into a project plan.

This project was approached from the perspective of, *"If I was hired at a company, what would my plan be to start from nothing to get a company to where it could pass an assessment?"* All of the CMMC practices and processes are addressed within the CMMC Kill Chain, but it is clear that the prioritization and "bucketing" of practices into phases is a subjective endeavor and not everyone may agree with this approach. Just understand that every organization is different and you will invariably need to modify the approach to fit your specific needs.

CONTRIBUTORS

Special thanks to the following contributors for the updated version of the CMMC Kill Chain:

Tom Cornelius
Senior Partner, ComplianceForge

Ryan Bonner
Founder and CEO, DEFCERT

Applying The Kill Chain Model To CMMC

You might be asking yourself how a kill chain model applies to CMMC. The root issue that is being addressed pertains to how many IT & cybersecurity professionals who are looking at the near future with dread. These front-line IT/cybersecurity practitioners currently do not know where to start, let alone what path they need to follow to pass a CMMC assessment.

There is an abundance of "*What is CMMC?*" guidance on LinkedIn, webinars and on the Internet in general, but there is a lack of practical guidance of HOW you are actually supposed to "*do CMMC*" in realistic terms. The CMMC Kill Chain is designed to provide a roadmap that would be usable for (1) anyone starting out or (2) anyone wanting to double check their approach. This model will also be added to the CMMC Center of Awesomeness website if you are looking for it in the future.

You can also download the graphic by clicking on the image below to get a PDF version of the graphic and description.

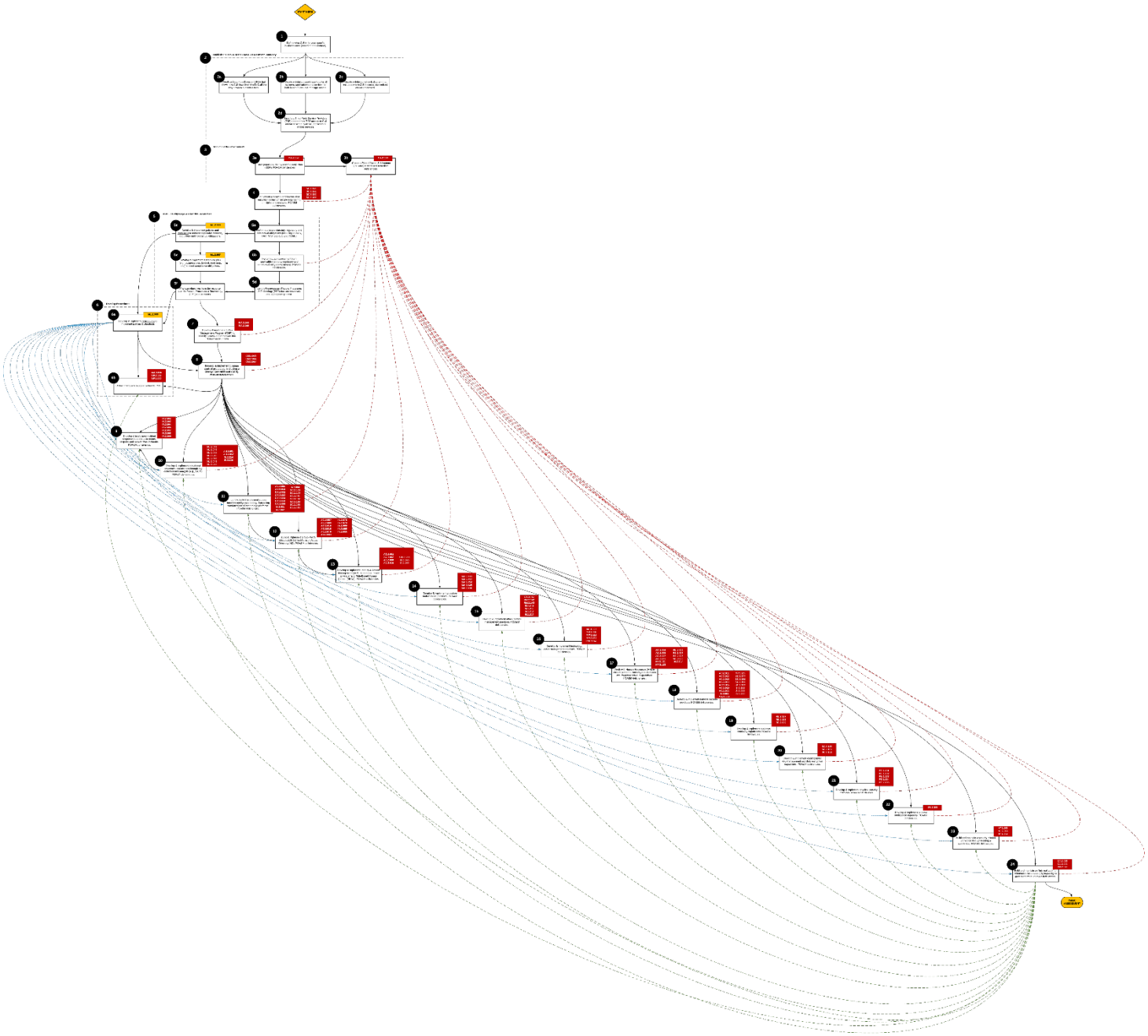


Image is downloadable from https://complianceforge.com/content/pdf/kill-chain-diagram-cmmc.pdf

Critical Resources & Acquisition Path (CRAP) - CMMC Project Planning Tool

The premise of the CMMC Kill Chain is to build a viable project plan from the perspective of a prioritized listing of tasks in order to successfully prepare for and pass a CMMC assessment. This helps establish your Critical Resources & Acquisition Path (CRAP), since errors or misguided adventures with people, processes and technology earlier in CMMC practice/process implementation activities will have cascading effects, so the CMMC Kill Chain is meant to provide a model for prioritizing CMMC-related pre-assessment activities.

The CMMC Kill Chain breaks down CMMC into 23 major steps, which can then be translated into a project plan.

Theory of Constraints – Managing Your CRAP

As with any process, an organization's CMMC compliance program is always vulnerable due to the ability of the "weakest link" (e.g., person, part, supplier and/or process) to cause damage and adversely affect the overall CMMC compliance program.

The theory of constraints (**TOC**) is a management paradigm that views any manageable system as being limited in achieving more of its goals by a very small number of constraints. There is always at least one constraint in a project/initiative and TOC utilizes a process to identify the constraint(s) and restructure the rest of the organization/processes around it.

CRAP Management Focus

At the management level, TOC focuses on:

- Define business processes;
- Establish minimum quality requirements for people, processes and technologies;
- Establish, review and enforce contract requirements;
- Appropriately resource technical requirements; and
- Maintain situational awareness.

CRAP Technical Focus

At the individual contributor level (e.g., analyst, engineer, technician, etc.), TOC focuses on:

- Define technical requirements;
- Identify and implement "industry recognized practices" to design, build and maintain systems, applications and services; and
- Provide metrics to management to maintain situational awareness.

Change Management Within CMMC

As you work through CMMC practices and processes, it is common that new technology solutions are necessary. This is inevitable and your organization may need to re-factor the CMMC Kill Chain as guidance for time and resource constraints.

There are several factors that need to be considered when incorporating new technologies:

1. Define the necessary technology solution(s) by identifying the necessary People, Processes & Technology (**PPT**).
2. Identify suitable vendors based on the vendor's:
    a. Knowledge of your statutory, regulatory, and contractual obligations;
    b. Ability to fill gaps related to those obligations; and
    c. Ability to "speak CMMC" (you want to avoid paying someone to be their Guinea pig to learn how to implement CMMC through on-the-job training).
3. Without exception, leverage your organization's change control processes to ensure the technology solutions are documented, reviewed and approved.
4. Leverage the CMMC Kill Chain phases to identify where you will implement and operate the new technology solution to understand possible "cascading effects" of new technologies on other phases. For example:

a. Your organization will see a direct impact from a Security Information and Event Management (SIEM) tool during the following CMMC Kill Chain phases:
    i. *10. Situational Awareness;*
    ii. *11. Baseline Security Configurations;*
    iii. *12. Centralized Controls Management;*
    iv. *13. Identity & Access Management;*
    v. *15. Vulnerability Management;*
    vi. *17. Personnel Security; and*
    vii. *18. Network Security.*
b. Your organization will see a direct impact from a security configuration / vulnerability scanning tool during the following CMMC Kill Chain phases:
    i. *8. Change Management;*
    ii. *11. Baseline Security Configurations; and*
    iii. *13. Vulnerability Management.*
c. Your organization will see a direct impact from an Application Control tool during the following CMMC Kill Chain phases:
    i. *11. Baseline Security Configurations; and*
    ii. *13. Identity & Access Management.*

5. Whenever multiple technology implementations overlap in a CMMC Kill Chain phase, be aware of time and resource constraints.
    a. Add time allowances for the procurement, training, configuration and ongoing operation of the new technology solution;
    b. Plan for the possibility that overlapping implementations may:
        i. Extend the time spent in a particular phase of the CMMC Kill Chain; and
        ii. Increase labor-related expenses:
            1. Professional services from the vendor or managed IT service providers familiar with the solution; and/or
            2. Technical staff support from another internal team.
6. Integrate new technologies into internal audit practices to maintain your Information Assurance (IA) capability and controls governance.
    a. This is the optimal time to develop performance measures (e.g., metrics) for assessing the continued effectiveness of your newly-implemented technology solutions.

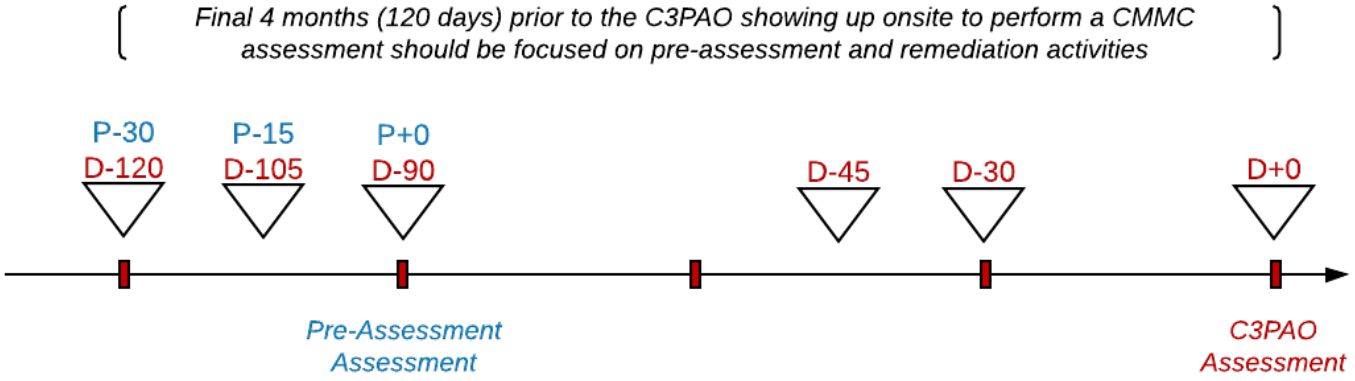
Background On The Logic Used In The CMMC Kill Chain

Here is a quick explanation on some of the reasoning used for this model:

- You can't legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management and a defined risk threshold. Risk management is the key building block that other practices rely upon.
- 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).
- From there, the assumption is that you will discover issues so incident response capability needs to exist (note - DFARS incident reporting requirements already apply if you currently store, process and/or transmit CUI as part of a DoD contract).
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.

Timeline Planning

It is critical to perform backwards planning for CMMC since the steps necessary to remediate gaps and correct false assumptions takes time. "D-Day" is when CMMC Third-Party Assessor Organization (**C3PAO**) assessors will be on-site to perform the CMMC assessment.



When viewed from a backwards planning perspective, you can realistically expect four months of "final cleanup" to validate assumptions and correct minor deficiencies:

- **D-0**. This is the day of the C3PAO assessment.
- **D-30**. One month prior to the assessment, tabletops/validation/proofs should be performed to finalize any remediate efforts.
- **D-45**. 6 weeks prior to the assessment, no new documentation / major changes should occur (e.g., change freeze).
- **D-90/P-0**. 3 months prior to the C3PAO assessment, you should conduct a pre-assessment (e.g., full-dress rehearsal).
- **D-105/P-15**. 2 weeks prior to the pre-assessment, tabletops/validation/proofs should be performed to validate assumptions.
- **D-120/P-30**. 1 month prior to the pre-assessment, no new documentation / major changes should occur (e.g., change freeze).

Pre-Assessment Assessment (PAA) Activities

The PAA should be viewed as a "full dress rehearsal" to validate evidence of due diligence and due care exists to successfully pass a C3PAO assessment:

- **P-30**. 4 months prior to the C3PAO assessment, no new documentation / major changes should occur (e.g., change freeze) to prepare for the PAA.
- **P-15**. 3.5 months prior to the C3PAO assessment, tabletops/validation/proofs should be performed to validate assumptions to prepare for the PAA.
- **P-0**. 3 months prior to the assessment the "full-dress rehearsal" assessment is performed to identify deficiencies, so there is ample time to implement appropriate remediation efforts prior to the formal C3PAO assessment.

C3PAO Assessment Activities

When the C3PAO assessors arrive on-site, all POA&M items must be remediated. Clear documentation that provides appropriate evidence of due diligence and due care must be correct and available:

- **D-45**. 6 weeks prior to the C3PAO assessment, no new documentation / major changes should occur (e.g., change freeze).
- **D-30**. One month prior to the C3PAO assessment, tabletops/validation/proofs should be performed to finalize any remediate efforts.
- **D-0**. This is the day of the C3PAO assessment.

CMMC Kill Chain Phases

The CMMC Kill Chain is made up of 23 phases (these correspond to the picture diagram from page 4):

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.

2. Define Scoping.

This has four subcomponent steps to define the scope of the CMMC assessment boundary:

a) Create a Data Flow Diagram (**DFD**) that shows how CUI flows from the DoD all the way down to subcontractors;
b) Create a detailed asset inventory for all systems, applications and services for both in-scope and out-of-scope assets;
c) Create a detailed network diagram that includes where CUI is stored, transmitted and/or processed; and
d) Inventory Third-Party Service Providers (**TSP**) to determine TSP access to CUI and/or in-scope systems, applications and/or services.

3. Documentation.

This has two subcomponent steps to document the CUI environment:

a) Start populating the System Security Plan (**SSP**); and
b) Create a Plan of Action & Milestone (**POA&M**) to track and remediate deficiencies.

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.

5. Resource Prioritization.

This has six subcomponent steps to plan, identify gaps and prioritize resources:

a) Define applicable statutory, regulatory and contractual obligations (including DFARS, FAR, NIST 800-171 and CMMC);
b) Perform a gap assessment from applicable statutory, regulatory and contractual obligations;
c) Develop & implement policies and standards to address applicable statutory, regulatory and contractual obligations;
d) Identify the necessary People, Processes & Technology (**PPT**) that are necessary and appropriately sized;
e) Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet compliance obligations; and
f) Prioritize objectives from the resource plan for PPT requirements. POA&M any deficiencies from this phase.

6. Procedures / Rules of Behavior.

This has two subcomponent steps:

a) Develop & implement procedures to implement policies & standards; and
b) Define processes to securely handle CUI. POA&M any deficiencies from this phase.

7. Risk Management.

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

8. Change Management.

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

23. Internal Audit.

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

Kill Chain #	Kill Chain Category	CMMC 2.0 Practice #	NIST SP 800-171 Control #	NIST SP 800-171 R2 Control
3	Documentation	CA.L2-3.12.2	3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
		CA.L2-3.12.4	3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.
4	Secure Architecture	SC.L1-3.13.1	3.13.1	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
		SC.L1-3.13.5	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
		SC.L2-3.13.2	3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
		SC.L2-3.13.6	3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
6	Procedures / Rules of Behavior	MP.L2-3.8.1	3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
		MP.L2-3.8.2	3.8.2	Limit access to CUI on system media to authorized users.
8	Change Management	CM.L2-3.4.3	3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.
		CM.L2-3.4.4	3.4.4	Analyze the security impact of changes prior to implementation.
		CM.L2-3.4.5	3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.
9	Incident Response Operations	IR.L2-3.6.1	3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
		IR.L2-3.6.2	3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
		IR.L2-3.6.3	3.6.3	Test the organizational incident response capability.
10	Situational Awareness	AU.L2-3.3.1	3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.
		AU.L2-3.3.2	3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.
		AU.L2-3.3.3	3.3.3	Review and update logged events.

		AU.L2-3.3.4	3.3.4	Alert in the event of an audit logging process failure.
		AU.L2-3.3.5	3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
		AU.L2-3.3.6	3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.
		AU.L2-3.3.8	3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
		SI.L2-3.14.3	3.14.3	Monitor system security alerts and advisories and take action in response.
		SI.L2-3.14.6	3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
11	Baseline Security Configurations	AC.L2-3.1.21	3.1.21	Limit use of portable storage devices on external systems.
		AU.L2-3.3.9	3.3.9	Limit management of audit logging functionality to a subset of privileged users.
		CM.L2-3.4.1	3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
		CM.L2-3.4.2	3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.
		CM.L2-3.4.6	3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
		CM.L2-3.4.7	3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.
		CM.L2-3.4.8	3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
		IA.L2-3.5.10	3.5.10	Store and transmit only cryptographically- protected passwords.
		IA.L2-3.5.11	3.5.11	Obscure feedback of authentication information.
		IA.L2-3.5.4	3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
		SC.L2-3.13.12	3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
		SC.L2-3.13.13	3.13.13	Control and monitor the use of mobile code.
		SC.L2-3.13.14	3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
		SC.L2-3.13.3	3.13.3	Separate user functionality from system management functionality.
		SC.L2-3.13.4	3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.
		SC.L2-3.13.9	3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
12		AC.L2-3.1.10	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.

	Centralized Controls Management	AC.L2-3.1.11	3.1.11	Terminate (automatically) a user session after a defined condition.
		AC.L2-3.1.5	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
		AC.L2-3.1.7	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
		AC.L2-3.1.8	3.1.8	Limit unsuccessful logon attempts.
		AU.L2-3.3.7	3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.
		IA.L2-3.5.5	3.5.5	Prevent reuse of identifiers for a defined period.
		IA.L2-3.5.6	3.5.6	Disable identifiers after a defined period of inactivity.
		IA.L2-3.5.7	3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.
		IA.L2-3.5.8	3.5.8	Prohibit password reuse for a specified number of generations.
		IA.L2-3.5.9	3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.
13	Identity & Access Management (IAM)	AC.L1-3.1.1	3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
		AC.L1-3.1.2	3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
		AC.L2-3.1.3	3.1.3	Control the flow of CUI in accordance with approved authorizations.
		AC.L2-3.1.6	3.1.6	Use non-privileged accounts or roles when accessing non-security functions.
		CM.L2-3.4.9	3.4.9	Control and monitor user-installed software.
		IA.L1-3.5.1	3.5.1	Identify system users, processes acting on behalf of users, and devices.
		IA.L1-3.5.2	3.5.2	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
14	Maintenance	MA.L2-3.7.1	3.7.1	Perform maintenance on organizational systems.
		MA.L2-3.7.2	3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
		MA.L2-3.7.3	3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
		MA.L2-3.7.4	3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
		MA.L2-3.7.6	3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.
15	Vulnerability Management	RM.L2-3.11.2	3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
		RM.L2-3.11.3	3.11.3	Remediate vulnerabilities in accordance with risk assessments.

		SI.L1-3.14.1	3.14.1	Identify, report, and correct system flaws in a timely manner.
		SI.L1-3.14.2	3.14.2	Provide protection from malicious code at designated locations within organizational systems.
		SI.L1-3.14.4	3.14.4	Update malicious code protection mechanisms when new releases are available.
		SI.L1-3.14.5	3.14.5	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
16	Asset Management	AC.L1-3.1.20	3.1.20	Verify and control/limit connections to and use of external systems.
		MP.L1-3.8.3	3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.
		MP.L2-3.8.4	3.8.4	Mark media with necessary CUI markings and distribution limitations.
		MP.L2-3.8.5	3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
17	Personnel Security	AC.L1-3.1.22	3.1.22	Control CUI posted or processed on publicly accessible systems.
		AC.L2-3.1.15	3.1.15	Authorize remote execution of privileged commands and remote access to security- relevant information.
		AC.L2-3.1.4	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
		AC.L2-3.1.9	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.
		MP.L2-3.8.7	3.8.7	Control the use of removable media on system components.
		MP.L2-3.8.8	3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.
		PE.L2-3.10.6	3.10.6	Enforce safeguarding measures for CUI at alternate work sites.
		PS.L2-3.9.1	3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.
		PS.L2-3.9.2	3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.
		SI.L2-3.14.7	3.14.7	Identify unauthorized use of organizational systems
18	Network Security	AC.L2-3.1.12	3.1.12	Monitor and control remote access sessions.
		AC.L2-3.1.13	3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
		AC.L2-3.1.14	3.1.14	Route remote access via managed access control points.
		AC.L2-3.1.16	3.1.16	Authorize wireless access prior to allowing such connections.
		AC.L2-3.1.17	3.1.17	Protect wireless access using authentication and encryption.
		AC.L2-3.1.18	3.1.18	Control connection of mobile devices.
		AC.L2-3.1.19	3.1.19	Encrypt CUI on mobile devices and mobile computing platforms

		IA.L2-3.5.3	3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.
		MA.L2-3.7.5	3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
		MP.L2-3.8.6	3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
		SC.L2-3.13.11	3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
		SC.L2-3.13.15	3.13.15	Protect the authenticity of communications sessions.
		SC.L2-3.13.7	3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).
19	Business Continuity	MP.L2-3.8.9	3.8.9	Protect the confidentiality of backup CUI at storage locations.
20	Encryption	SC.L2-3.13.10	3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.
		SC.L2-3.13.16	3.13.16	Protect the confidentiality of CUI at rest.
		SC.L2-3.13.8	3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
21	Physical Security	PE.L1-3.10.1	3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
		PE.L1-3.10.3	3.10.3	Escort visitors and monitor visitor activity.
		PE.L1-3.10.4	3.10.4	Maintain audit logs of physical access.
		PE.L1-3.10.5	3.10.5	Control and manage physical access devices.
		PE.L2-3.10.2	3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.
22	Security Awareness Training	AT.L2-3.2.1	3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
		AT.L2-3.2.2	3.2.2	Ensure that personnel are trained to carry out their assigned information security- related duties and responsibilities.
		AT.L2-3.2.3	3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.
23	Internal Audit	CA.L2-3.12.1	3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
		CA.L2-3.12.3	3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
		RM.L2-3.11.1	3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

APPENDIX A – DOCUMENTATION TO SUPPORT NIST 800-171 COMPLIANCE & CMMC

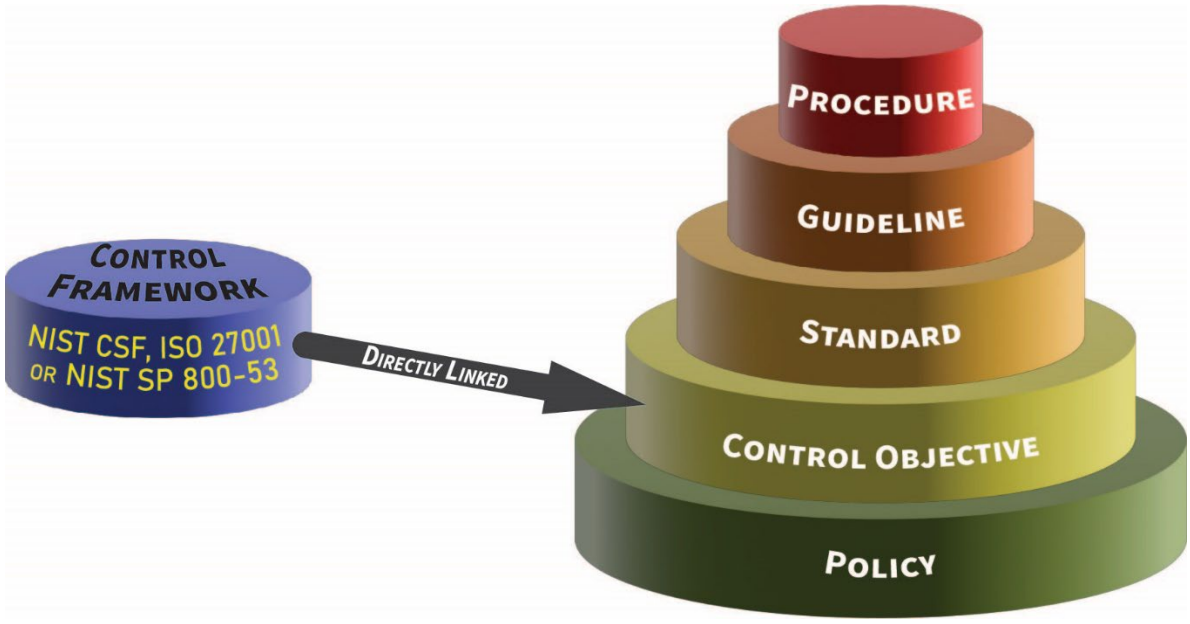
The purpose of a company's cybersecurity documentation is to prescribe a comprehensive framework for:

- Creating a clearly articulated approach to how your company handles cybersecurity.
- Protecting the confidentiality, integrity, availability and safety of data and systems on your network.
- Providing guidance to help ensure the effectiveness of security controls that are put in place to support your company's operations.
- Helping your users to recognize the highly-networked nature of the current computing environment to provide effective company-wide management and oversight of those related cybersecurity risks.

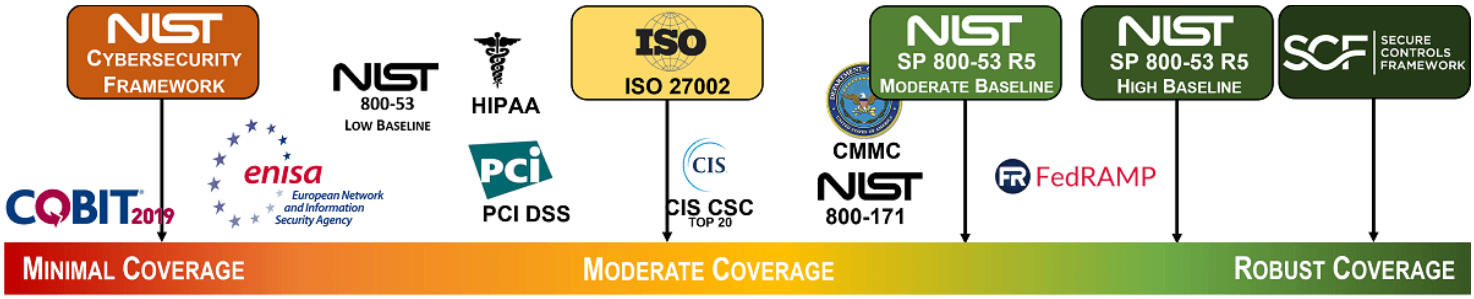
Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for individuals / teams to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off the policy and those supporting components also build off each other to make a cohesive and scalable approach to addressing a requirement.

Well-designed **NIST 800-171 / CMMC documentation** is comprised of six (6) core components:

(1) Policies that establish management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
(6) Guidelines are recommended, but not mandatory.



Note - From a framework perspective, NIST 800-171 is more closely aligned with NIST 800-53 than others. This falls in more of a "moderate" category for cybersecurity controls, which would be reasonably-expected in nearly any industry.



BREADTH & DEPTH OF CYBERSECURITY & PRIVACY CONTROLS

NIST 800-171 In a Nutshell

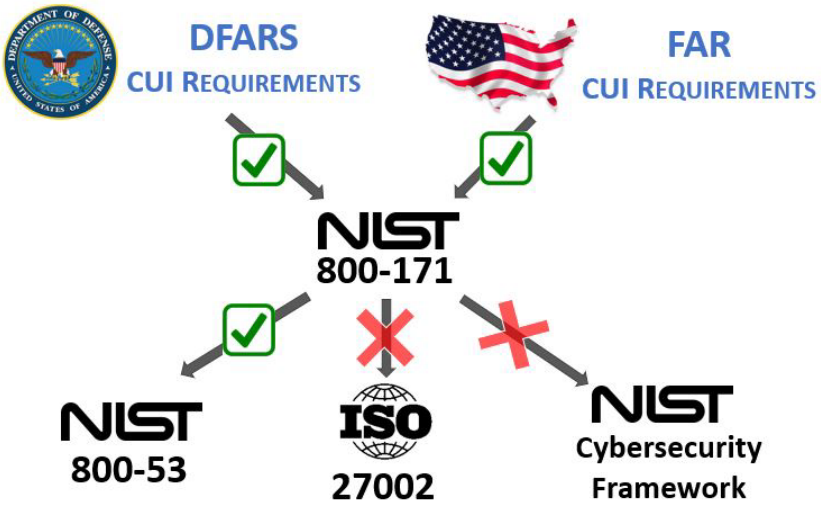
When you break down NIST 800-171 CUI/FCI requirements into how they are operationalized by people, processes or technology, you see that there are a lot of controls that are either administrative or related to technical configurations. Very few realistically require the purchase of new hardware or software to meet these compliance requirements, so NIST 800-171 accomplished through improving processes and configuring existing technologies to meet compliance requirements.

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

Administrative (e.g., policies, standards & procedures)
Technical Configurations(e.g., security settings)
Software Solution
Hardware Solution
Software or Hardware Solution
Assigned Tasks To Cybersecurity Personnel
Assigned Tasks To IT Personnel
Assigned Tasks To Application/Asset/Process Owner
Configuration or Software Solution
Configuration or Software or Hardware or Outsourced Solution

NIST 800-171 Specific Documentation

When you look at NIST 800-171, it contains mappings to both NIST 800-53 and ISO 27002. Only NIST 800-53 controls provide complete mapping to the NIST 800-171 CUI/FCI and NFO controls, so NIST 800-53 should serve as the aligned framework when building your organization's cybersecurity documentation. The NIST Cybersecurity Framework would be considered too lightweight to address NIST 800-171 compliance obligations.



Cybersecurity Documentation Hierarchy – Understanding How Cybersecurity Documentation Is Connected

It all starts with influencers – these influencers set the tone and establish what is considered to be due care for information security operations. For external influencers, this includes statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding agreements) that companies must address. For internal influencers, these are business-driven and the focus is more on management's desire for consistent, efficient and effective operations.

When that is all laid out properly, your company's cybersecurity documentation show flow like this where your policies are linked all the way down to metrics: https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf