COMPLIANCE FORGE

CMMC Kill Chain

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

Version 2020.1

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 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 24 major steps, which can then be translated into a project plan.

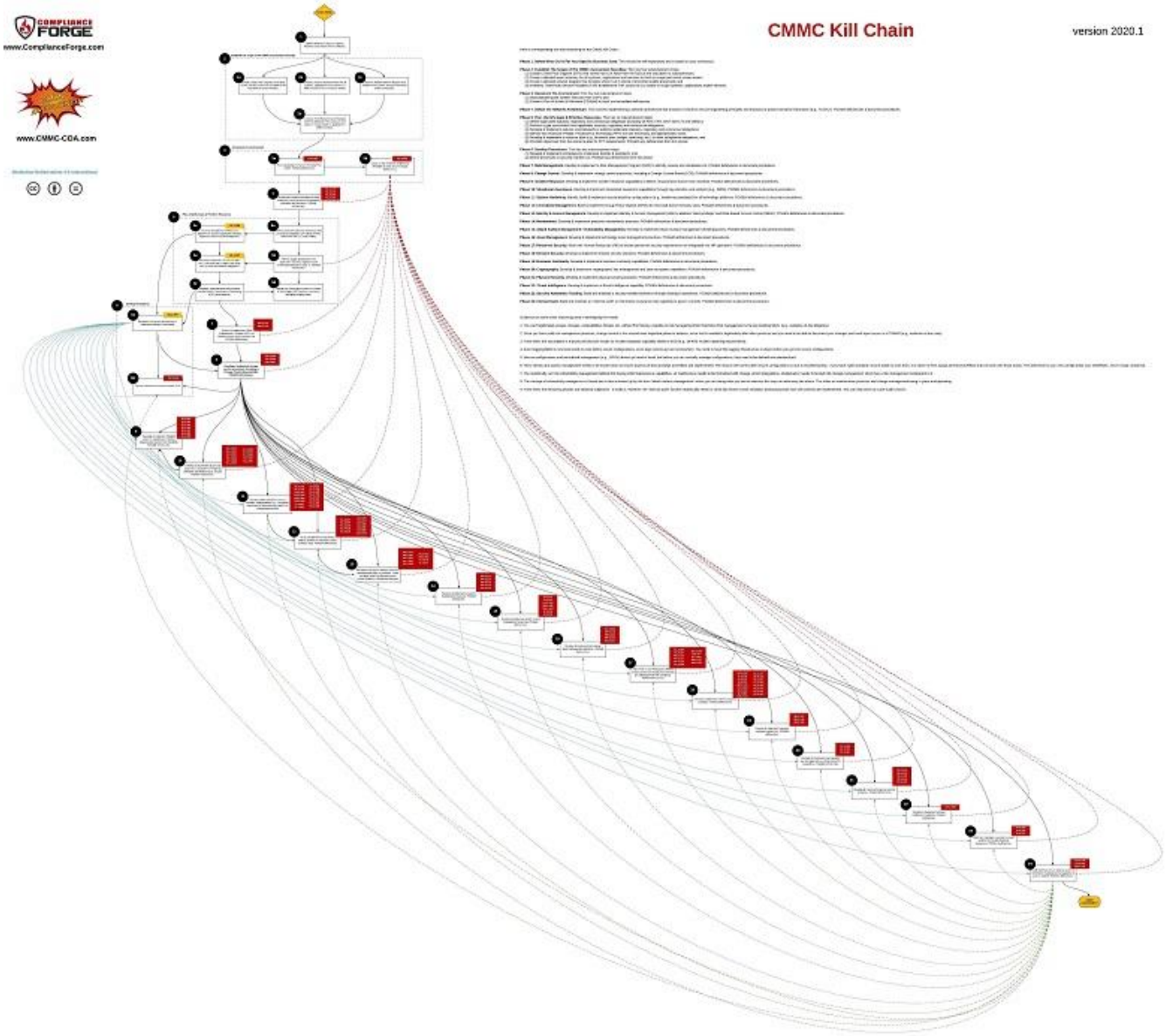
This project was approached from the perspective of, “If I was hired at a company, what would my plan be to start from nothing to get a company to where it could pass an assessment?” All of the CMMC practices and processes are addressed within the CMMC Kill Chain, but it is clear that the prioritization 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.

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 2021 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 it by clicking on the image below to get a PDF version of the graphic and description.



[image is downloadable from http://www.cmmc-kill-chain.com]

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. 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 24 major steps, which can then be translated into a project plan.

CMMC Kill Chain Phases

The CMMC Kill Chain is made up of 24 phases (these correspond to the picture diagram):

1. **Define What CUI Is For Your Specific Business Case**. This should be self-explanatory and is based on your contract(s).

2. **Establish The Scope of The CMMC Assessment Boundary**. This has four subcomponent steps:
   (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.

3. **Document The Environment**. This has two subcomponent steps:
   (1) Start populating the System Security Plan (SSP); and
   (2) Create a Plan of Action & Milestone (POA&M) to track and remediate deficiencies.

4. **Define The Network 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. **Plan, Identify Gaps & Prioritize Resources**. This has six subcomponent steps:
   (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.

6. **Develop Procedures**. 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.

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

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

9. **Incident Response**. 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. **System Hardening**. Identify, build & implement secure baseline configurations (e.g., hardening standards) for all technology platforms. POA&M deficiencies & document procedures.

12. **Centralized 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. **Attack Surface Management / 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. **Cryptography**. 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. **Threat Intelligence**. Develop & implement a threat intelligence capability. POA&M deficiencies & document procedures.

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

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

BACKGROUND ON THE LOGIC USED IN THIS MODEL

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

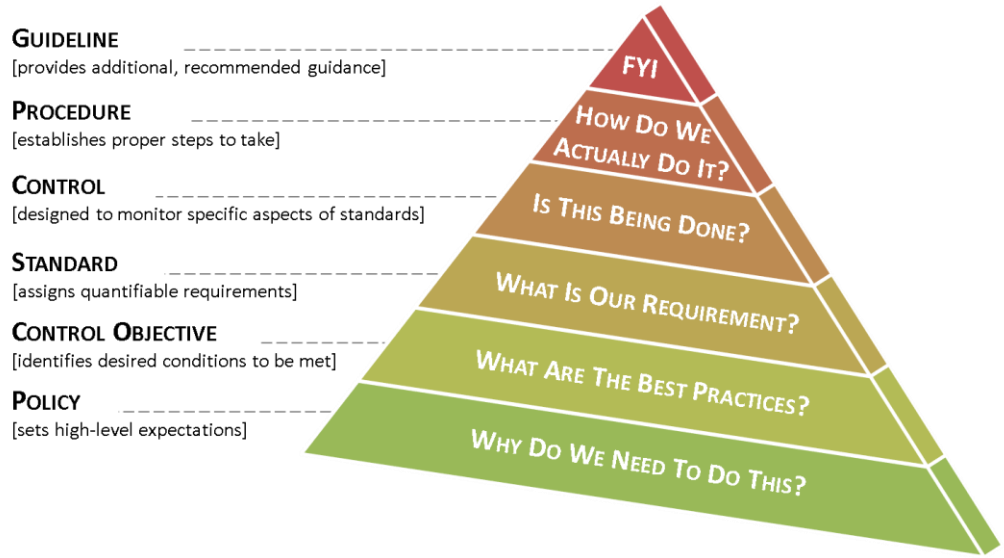
- You can't legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management and a defined risk threshold. Risk management is the key building block that other practices rely upon.
- Once you have solid risk management practices, change control is the second 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.

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 users to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off of the policy and all of the components of cybersecurity documentation build off each other to make a cohesive approach to addressing a requirement:



CYBERSECURITY DOCUMENTATION COMPONENTS

Cybersecurity documentation is comprised of six (6) main parts:

(1) Core policy that establishes 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.

NIST 800-171 In a Nutshell

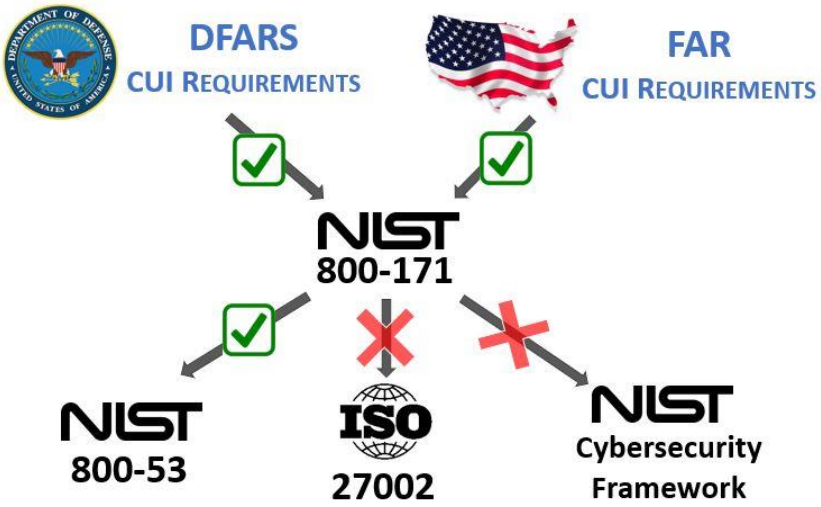
When you break down NIST 800-171 CUI/FCI requirements into how they are operationalized by people, processes or technology, you see that there are a lot of controls that are either administrative or related to technical configurations. Very few realistically require the purchase of new hardware or software 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*

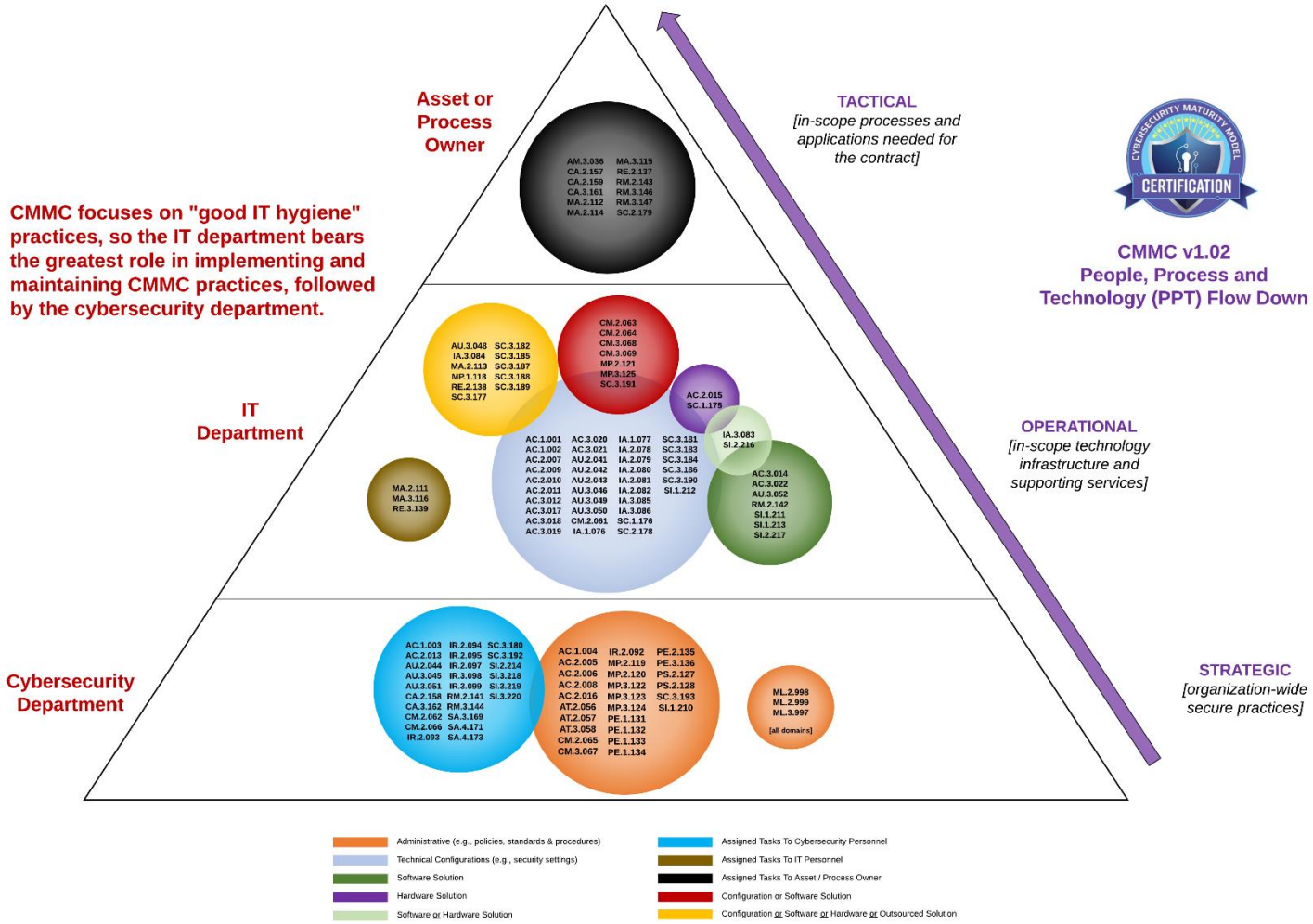
NIST 800-171 Specific Documentation

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 to lightweight to address NIST 800-171 compliance obligations.



CONTROL / PRACTICE STAKEHOLDERS

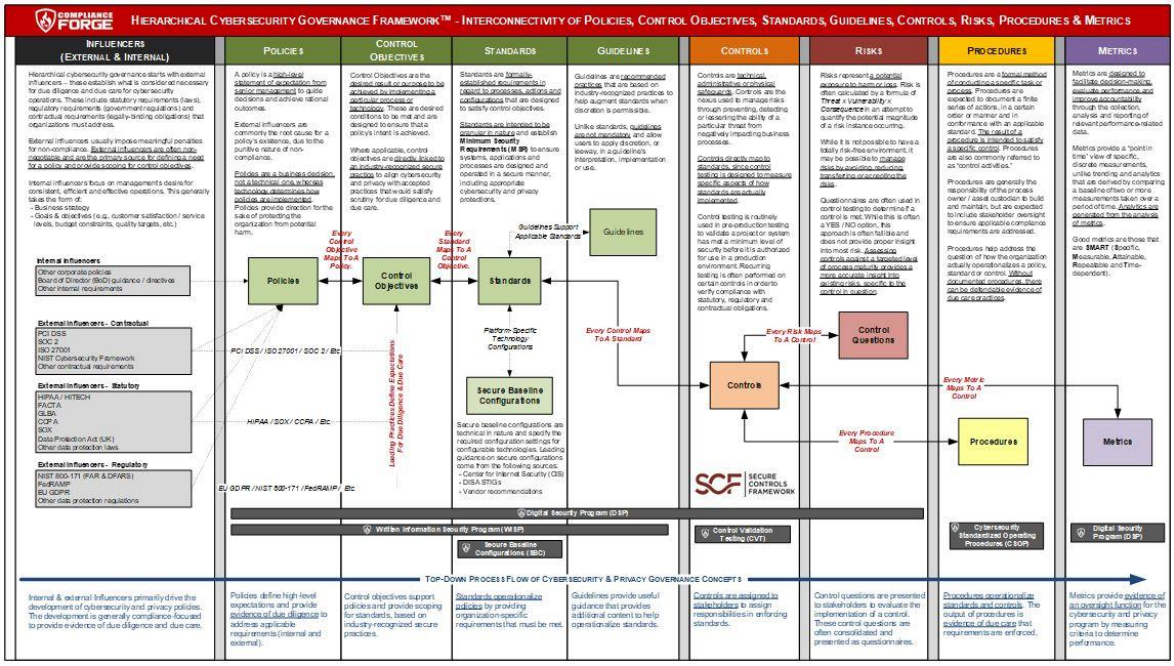
It is important for anyone getting started with NIST 800-171 / CMMC to first understand who the stakeholders are. As you can see from the diagram below, the majority of the practices/controls are "owned" by the IT department, with quite a few being the responsibility of the asset/process owner. This is where the cybersecurity team needs to educate all applicable stakeholders on their roles and responsibilities for NIST 800-171 / CMMC compliance obligations.



Cybersecurity Documentation Hierarchy – Understanding How Cybersecurity Documentation Is Connected

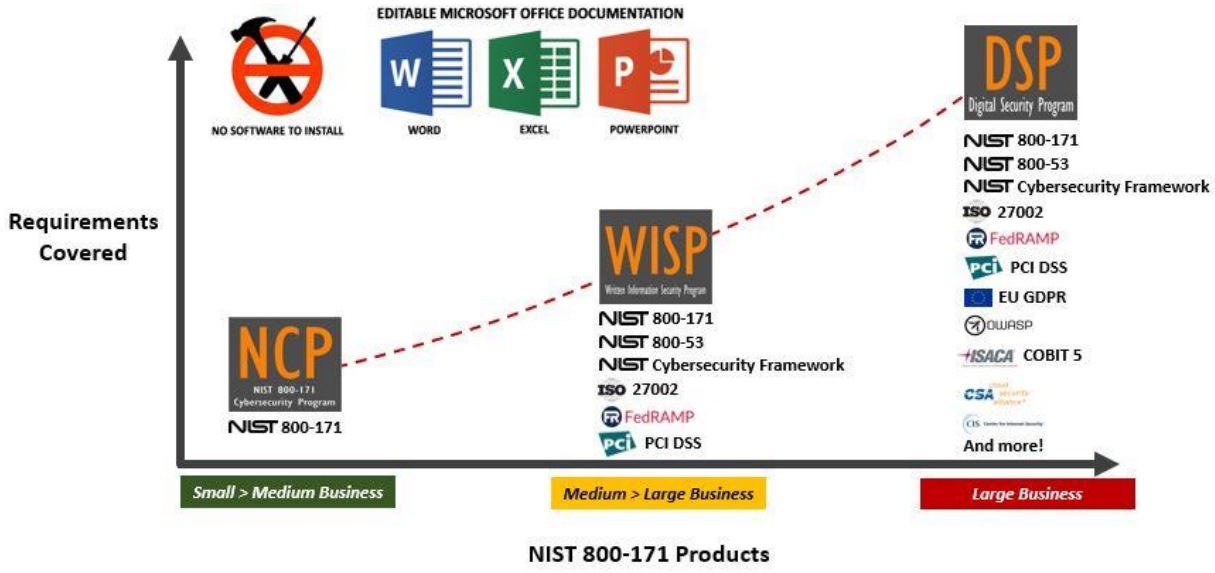
It all starts with influencers – these influencers set the tone and establish what is considered to be due care for information security operations. For external influencers, this includes statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding 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:
http://examples.complianceforge.com/ComplianceForge%20Hierarchical%20Cybersecurity%20Governance%20Framework.pdf



ComplianceForge sells several different options for NIST 800-171 compliance documentation, based on your needs:

- **NIST 800-171 Compliance Program (NCP)** – designed for smaller organizations;
- **Written Information Security Program (WISP)** – designed for organizations that want to closely align with NIST 800-53; and
- **Digital Security Program (DSP)** – enterprise solution for organizations that need to comply with a wide variety of requirements.



Example NIST 800-171 Cybersecurity Documentation

Complying with the requirements from DFARS goes beyond just having policies and standards. When you break down the requirements to comply with NIST 800-171, you see how ComplianceForge's products address a specific DFARS/NIST 800-171 compliance need. In the chart, "NFO" stands for Non-Federal Organization. NFO controls are required for contractors and are called out in Appendix E of NIST 800-171.

Below are examples of how a cybersecurity documentation should look for NIST 800-171 compliance:

ComplianceForge Product	DFARS Requirement
Written Information Security Program (WISP); NIST 800-171 Compliance Program (NCP) or Digital Security Program (DSP) [addresses high-level policies & standards]	252.204-7008 252.204-7012 **NIST 800-171 (multiple NFO controls)**
Cybersecurity Standardized Operating Procedures (CSOP)	252.204-7008 252.204-7012 **NIST 800-171 (multiple NFO controls)**
Vendor Compliance Program (VCP)	252.204-7008 252.204-7012 **NIST 800-171 NFO PS-7**
Cybersecurity Risk Management Program (RMP)	252.204-7008 252.204-7012 **NIST 800-171 NFO RA-1**
Cybersecurity Risk Assessment Template (CRA)	252.204-7008 252.204-7012 **NIST 800-171 3.11.1**
Vulnerability & Patch Management Program (VPMP)	252.204-7008 252.204-7012 **NIST 800-171 3.11.2**
Integrated Incident Response Program (IIRP)	252.204-7008 252.204-7009 252.204-7010 252.204-7012 **NIST 800-171 3.6.1**
Security & Privacy By Design (SPBD)	252.204-7008 252.204-7012 **NIST 800-171 NFO SA-3**
System Security Plan (SSP)	252.204-7008 252.204-7012 **NIST 800-171 3.12.4**
Continuity of Operations Plan (COOP)	252.204-7008 252.204-7012 **NIST 800-171 3.6.1**
Secure Baseline Configurations (SBC)	252.204-7008 252.204-7012 **NIST 800-171 3.4.1**
Control Validation Testing (CVT)	252.204-7008 252.204-7012 **NIST 800-171 NFO CA-1**
Cybersecurity Business Plan (CBP)	CMMC CA.4.163