NIST 800-171 R3 Kill Chain

A Phase-Based Model To Prioritize NIST 800-171 R3 Control Implementation

Version 2024.1

Disclaimer: This document is provided for educational purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a competent cybersecurity and/or data privacy professional.

Table of Contents

EXECUTIVE SUMMARY

The concept of creating a "NIST 800-171 R3 Kill Chain" is to provide an efficient way to plan out a roadmap to successfully demonstrate compliance with NIST 800-171 R3. The result is a viable approach for anyone to use in order to create a prioritized project plan for NIST 800-171 R3 control implementation.

Why "NIST 800-171 R3 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 how the DoD's Cybersecurity Maturity Model Certification (CMMC) has 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 NIST 800-171 R3 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 NIST 800-171 R3 control implementation into 22 major steps, which can then be translated into a viable 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 a NIST 800-171 R3 assessment?"* All NIST 800-171 R3 controls are addressed within the NIST 800-171 R3 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 goes to the following contributors, since this document would not exist without their applied expertise:

Tom Cornelius
Senior Partner
ComplianceForge

Mark Allers
VP, Business Development
Cimcor

Ryan Bonner
Founder & CEO
Defcert

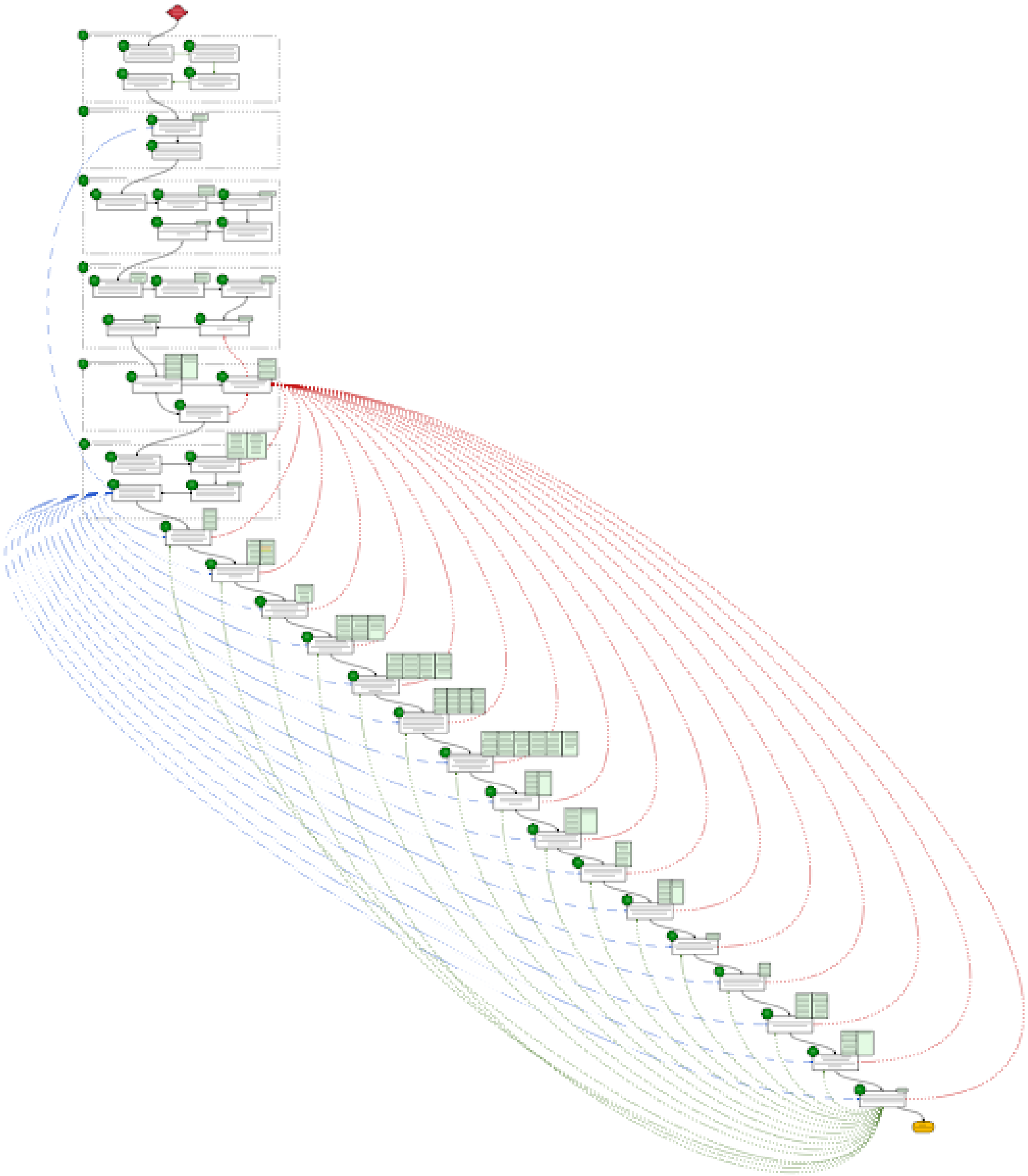
Tim Trickett
CTO, Public Sector
BDO

Applying The Kill Chain Model To NIST 800-171 & CMMC

You might be asking yourself how a kill chain model applies to NIST 800-171 R3 & Cybersecurity Maturity Model Certification (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 demonstrate compliance with NIST 800-171 R3 and eventually pass a future “CMMC 3.0” assessment.

There is an abundance of "*What is NIST 800-171?*" 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 NIST 800-171*" in realistic terms. The NIST 800-171 R3 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.[1]

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://content.complianceforge.com/NIST-800-171-R3-Kill-Chain-Overview.pdf]

[1] CMMC Center of Awesomeness – https://cmmc-coa.com

CRITICAL RESOURCES & ACQUISITION PATH (CRAP) – NIST 800-171 R3 PROJECT PLANNING

The premise of the NIST 800-171 R3 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 NIST 800-171 R3 controls assessment. This helps establish your Critical Resources & Acquisition Path (CRAP), since errors or misguided adventures with people, processes and technology earlier in NIST 800-171 R3 control implementation activities will have cascading effects, so the NIST 800-171 R3 Kill Chain is meant to provide a model for prioritizing NIST 800-171-related pre-assessment activities.

The NIST 800-171 R3 Kill Chain breaks down NIST 800-171 R3 control implementation into 22 major steps, which can then be translated into a viable project plan.

THEORY OF CONSTRAINTS (TOC) – 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.

OPERATIONALIZING CRAP TO YOUR BENEFIT

This concept of the TOC/CRAP is operationalized through the NIST 800-171 R3 Kill Chain in multiple scenarios:

- As an assessment readiness exercise;
- Prioritization decisions for a phased implementation plan; and
- As a method for introducing a new tool or capability into an existing environment.

"Knowing your CRAP" fundamentally comes down to clearly distinguishing between facts and assumptions. This is the premise for compliance decision making.

Facts are statements of truth, or statements thought to be true. For example:

- The organization stores and processes Controlled Unclassified Information (CUI) as part of a government contract.
- NIST SP 800-171 compliance has been a requirement since 1 January 2018.
- NIST SP 800 171 R3 was released on 14 May 2024.
- The DoD issued a class deviation to delay DFARS implementation of NIST SP 800-171 R3.
- Office of Management and Budget (OMB) requires organizations to adopt the most current version of NIST one year after its release.

- Per 32 CFR § 170.19(c)(2), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).

Assumptions are essentially gaps in knowledge or information that need to be confirmed or denied. For example:

- Before NIST SP 800-171 R2 is deprecated in May 2025, the DoD will remove the class deviation for DFARS to transition to NIST SP 800-171 R3.
- The DoD may realize that the Defense Industrial Base (DIB) would be under undo financial pressure to adjust its technologies, ESP and business processes to treat SPD as CUI.

Change Management CRAP Considerations For NIST 800-171 R3

As you work through NIST 800-171 R3 controls, it is likely that new technologies and/or processes may be necessary. Technology change is inevitable and your organization may need to adjust the NIST 800-171 R3 Kill Chain for your specific needs and circumstances.

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, Data & Facilities (**PPTDF**).
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 NIST 800-171 R3" (you want to avoid paying someone to be their Guinea pig to learn how to implement NIST 800-171 R3 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 NIST 800-171 R3 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 NIST 800-171 R3 Kill Chain phases:
      i. Phase 11. Situational Awareness;
      ii. Phase 12. Secure Baseline Configurations;
      iii. Phase 13. Identity & Access Management (IAM);
      iv. Phase 15. Attack Surface Management (Vulnerability Management); and
      v. Phase 17. Network Security.
   b. Your organization will see a direct impact from a security configuration / vulnerability scanning tool during the following NIST 800-171 R3 Kill Chain phases:
      i. Phase 7. Change Management (CM);
      ii. Phase 12. Secure Baseline Configurations; and
      iii. *Phase 15. Attack Surface Management (Vulnerability Management).*
   c. Your organization will see a direct impact from an Application Control tool during the following NIST 800-171 R3 Kill Chain phases:
      i. Phase 12. Secure Baseline Configurations; and
      ii. Phase 13. Identity & Access Management (IAM).
5. Whenever multiple technology implementations overlap in a NIST 800-171 R3 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; and
   b. Plan for the possibility that overlapping implementations may:
      i. Extend the time spent in a particular phase of the NIST 800-171 R3 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 (IA) practices to maintain your information assurance 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.

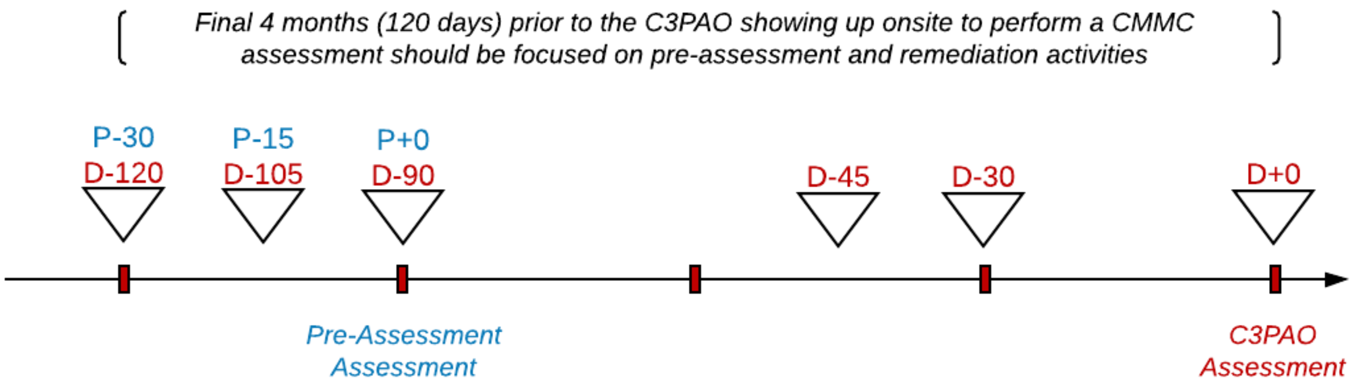
BACKGROUND ON THE LOGIC USED IN THE NIST 800-171 R3 KILL CHAIN

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

- If you fail to establish context (e.g., facts & assumptions), your entire premise for compliance operations may be incorrect and that could lead you down the wrong path. From a due diligence perspective, establishing context for cybersecurity and data protection should be a holistic endeavor to define all applicable laws, regulations and contractual obligations for cybersecurity and data protection. This enables your organization to implement proper governance practices (e.g., scope of compliance, stakeholders, supply chain protections, etc.).
- 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, it is necessary to have Change Management (CM) matured to a state where it supports IT and business processes. CM 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).
- Developing and implementing organization-wide data protection practices are crucial to limit logical and physical access to sensitive/regulated data (e.g., FCI, CUI, etc.). Technology is meant to follow practice, not the other way around where practices are modified to fit technology limitations. This means that technology should enable business practices to make the business more efficient, instead of technology solutions being implemented that hinder business practices.
- With the understanding of how business practices are meant to be supported, it should be possible to implement a segmented network architecture that can minimize the scope of compliance, while also supporting secure business practices.
- From there, the assumption is that you will discover issues so incident response capability needs to exist.
- Situational awareness (e.g., event logging, centralized/automated log review, etc.) s 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., STIGs, group policies, etc.) 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 Role Based Access Control (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 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 NIST 800-171 / CMMC assessments 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.


Final 4 months (120 days) prior to the C3PAO showing up onsite to perform a CMMC assessment should be focused on pre-assessment and remediation activities
P-30
D-120
P-15
D-105
P+0
D-90
D-45
D-30
D+0
Pre-Assessment Assessment
C3PAO 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.

NIST 800-171 R3 Kill Chain Phases

The NIST 800-171 R3 Kill Chain is made up of 22 phases (these correspond to the picture diagram from page 4):

1. Establish Context For Cybersecurity & Data Protection

If you fail to establish context (e.g., facts & assumptions), your entire premise for compliance operations may be incorrect and that could lead you down the wrong path. From a due diligence perspective, establishing context for cybersecurity and data protection should be a holistic endeavor to define all applicable laws, regulations and contractual obligations for cybersecurity and data protection. The reason for this is it is better to have a complete understanding of all requirements at the beginning to avoid reworking in the future, which sacrifices both time and resources.

This phase has four (4) sub-components:

a) Define the organization's applicable statutory, regulatory and contractual obligations for cybersecurity and data protection (e.g., DFARS, FAR, ITAR, etc.).
b) Define what Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI) is for your specific business case (based on the contract).
c) Identify the necessary People, Processes, Technology, Data & Facilities (PPTDF) that are necessary and appropriately sized.
d) Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to meet the organization's unique compliance obligations.

2. Implement Governance Practices

With an understanding of what needs protecting and those associated resources, it is possible to implement appropriate governance practices. This phase has two (2) sub-components:

a) Develop, implement and maintain policies and standards to address applicable statutory, regulatory and contractual obligations.
b) Prioritize objectives from the resource plan for People, Processes, Technology, Data & Facilities (PPTDF) requirements.

3. Establish The Compliance Scope

For most organization, there are both internal and external components that are in-scope for NIST 800-171. This phase focuses on eliminating assumptions by clearly documenting where CUI is stored, processed and/or transmitted, as well as developing an inventory of third-parties and their associated roles and responsibilities for protecting FCI/CUI. This phase has five (5) sub-components:

a) Create a Data Flow Diagram (DFD) that shows how CUI flows from the DoD all the way down to subcontractors.
b) Create and maintain 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.
d) Inventory External Service Providers (ESP) to determine ESP access to CUI and/or in-scope systems, applications and/or services.
e) Define roles and responsibilities for internal and external systems, applications and services.

4. Risk Management Practices

Risk management is the key building block that other practices rely upon. It is infeasible to govern changes and/or assess vulnerabilities, threats, etc. without first having established risk management practices. Risk management practices establish thresholds for acceptable risk for both internal and external stakeholders. This phase has five (5) sub-components:

a) Develop & implement an organization-wide Risk Management Program (RMP) to identify, assess and remediate risk. POA&M deficiencies to prioritize, resource and remediate.
b) Document and maintain a Cybersecurity Supply Chain Risk Management (C-SCRM) Plan that is specific to the CUI environment.
c) Develop and implement acquisition strategies, contract tools, and procurement methods to operationalize the C-SCRM Plan

d) Enforce C-SCRM requirements across the supply chain.
e) Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.

5. Document The CUI and/or FCI Environment

Documenting the CUI and/or FCI environment primarily focuses on populating the System Security Plan (SSP), which should be thought of as a "living document" where the SSP is never complete, since as changes occur throughout the System Develop Lifecycle (SDLC), the SSP also is updated to reflect current technologies, applicable controls and implementation status. This phase has three (3) sub-components:

a) Start populating the System Security Plan (SSP). POA&M deficiencies to prioritize, resource and remediate.
b) Create and maintain a Plan of Action & Milestone (POA&M) to track and remediate deficiencies.
c) Perform a gap assessment from applicable statutory, regulatory and contractual obligations. POA&M deficiencies to prioritize, resource and remediate.

6. Identify Compliance Stakeholders

Clearly defined roles and responsibilities are necessary to avoid improper assumptions. For external organizations, this requires contractual obligations to enforce those roles and responsibilities. This has two subcomponent steps:

a) Identify compliance stakeholders (including control owners and control operators) and formally assign those individuals roles and responsibilities. From a governance perspective, this can be simplified in a Responsible, Accountable, Supporting, Consulted and Informed (RASCI) matrix.
b) Work with Human Resources (HR) to ensure personnel security requirements are integrated into HR operations. POA&M deficiencies to prioritize, resource and remediate.
c) Define and implement processes to securely handle CUI wherever CUI is stored, processed and/or transmitted
d) Ensure control owners / operators develop, implement and maintain procedures to operationalize the organization's policies & standards.

POA&M deficiencies to prioritize, resource and remediate.

7. Data Protection Practices

This involves developing and implementing data protection practices to limit logical and physical access to CUI and/or FCI. POA&M deficiencies to prioritize, resource and remediate.

8. Segmented 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 to prioritize, resource and remediate.

9. Change Management (CM)

This involves developing and implementing Change Management (CM) practices, including a Change Control Board (CCB). POA&M deficiencies to prioritize, resource and remediate.

10. Incident Response (IR)

This involves developing and implementing Incident Response (IR) capabilities to detect, respond and recover from incidents (e.g., Incident Response Plan (IRP)). POA&M deficiencies to prioritize, resource and remediate.

11. Situational Awareness (SA)

This involves developing and implementing Situational Awareness (SA) capabilities through threat intelligence, log collection and analysis (e.g., SIEM, XDR, etc.). POA&M deficiencies to prioritize, resource and remediate.

12. Secure Baseline Configurations (SBC)

This involves developing and implementing Secure Baseline Configurations (SBC) (e.g., hardening standards) for all technology platforms (e.g., servers, workstations, network gear, applications, databases, etc.). POA&M deficiencies to prioritize, resource and remediate.

13. Identity & Access Management (IAM)

This involves developing and implementing Identity & Access Management (IAM) capabilities to address "least privilege" and Role-Based Access Control (RBAC). POA&M deficiencies to prioritize, resource and remediate.

14. Proactive Maintenance

This involves developing and implementing proactive maintenance practices. POA&M deficiencies to prioritize, resource and remediate.

15. Attack Surface Management (ASM)

This involves developing and implementing Attack Surface Management (ASM) practices to identify and remediate vulnerabilities. POA&M deficiencies to prioritize, resource and remediate.

16. IT Asset Management (ITAM)

This involves developing and implementing IT Technology Asset Management (ITAM) practices. POA&M deficiencies to prioritize, resource and remediate.

17. Layered Network Defenses

This involves developing and implementing layered network security for Defense-in-Depth (DiD) practices. POA&M deficiencies to prioritize, resource and remediate.

18. Business Continuity & Disaster Recovery (BC/DR)

This involves developing and implementing Business Continuity / Disaster Recovery (BC/DR) capabilities. POA&M deficiencies to prioritize, resource and remediate.

19. Cryptographic Key Management

This involves developing and implementing cryptographic key management and data encryption capabilities. POA&M deficiencies to prioritize, resource and remediate.

20. Physical Security

This involves developing and implementing physical security practices. POA&M deficiencies & document procedures.

21. Security Awareness Training

This involves developing and implementing training & awareness to ensure a security-minded workforce. POA&M deficiencies & document procedures. POA&M deficiencies to prioritize, resource and remediate.

22. Internal Audit (IA)

This involves developing and implementing an "internal audit" or Information Assurance (IA) capability to govern controls. POA&M deficiencies & document procedures. POA&M deficiencies to prioritize, resource and remediate.

Kill Chain #	Kill Chain Category	NIST 800-171 R3 Control #	NIST 800-171 R3 Control Name	NIST 800-171 R3 Control Description
N/A	N/A	03.01.01	Account Management	N/A
13	Identity & Access Management (IAM)	03.01.01.a	Account Management	Define the types of system accounts allowed and prohibited.
13	Identity & Access Management (IAM)	03.01.01.b	Account Management	Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.
13	Identity & Access Management (IAM)	03.01.01.c	Account Management	Specify:
13	Identity & Access Management (IAM)	03.01.01.c.01	Account Management	Authorized users of the system,
13	Identity & Access Management (IAM)	03.01.01.c.02	Account Management	Group and role membership, and
13	Identity & Access Management (IAM)	03.01.01.c.03	Account Management	Access authorizations (i.e., privileges) for each account.
13	Identity & Access Management (IAM)	03.01.01.d	Account Management	Authorize access to the system based on:
13	Identity & Access Management (IAM)	03.01.01.d.01	Account Management	A valid access authorization and
13	Identity & Access Management (IAM)	03.01.01.d.02	Account Management	Intended system usage.
13	Identity & Access Management (IAM)	03.01.01.e	Account Management	Monitor the use of system accounts.
13	Identity & Access Management (IAM)	03.01.01.f	Account Management	Disable system accounts when:
13	Identity & Access Management (IAM)	03.01.01.f.01	Account Management	The accounts have expired,
13	Identity & Access Management (IAM)	03.01.01.f.02	Account Management	The accounts have been inactive for [Assignment: organization-defined time period],
13	Identity & Access Management (IAM)	03.01.01.f.03	Account Management	The accounts are no longer associated with a user or individual,
13	Identity & Access Management (IAM)	03.01.01.f.04	Account Management	The accounts are in violation of organizational policy, or
13	Identity & Access Management (IAM)	03.01.01.f.05	Account Management	Significant risks associated with individuals are discovered.
13	Identity & Access Management (IAM)	03.01.01.g	Account Management	Notify account managers and designated personnel or roles within:
13	Identity & Access Management (IAM)	03.01.01.g.01	Account Management	[Assignment: organization-defined time period] when accounts are no longer required.
13	Identity & Access Management (IAM)	03.01.01.g.02	Account Management	[Assignment: organization-defined time period] when users are terminated or transferred.
13	Identity & Access Management (IAM)	03.01.01.g.03	Account Management	[Assignment: organization-defined time period] when system usage or the need-to-know changes for an individual.
13	Identity & Access Management (IAM)	03.01.01.h	Account Management	Require that users log out of the system after [Assignment: organization-defined time period] of expected inactivity or when [Assignment: organization-defined circumstances].
13	Identity & Access Management (IAM)	03.01.02	Access Enforcement	Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

8	Segmented Network Architecture	03.01.03	Information Flow Enforcement	Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.
N/A	N/A	03.01.04	Separation of Duties	N/A
6b	Identify Compliance Stakeholders	03.01.04.a	Separation of Duties	Identify the duties of individuals requiring separation.
6b	Identify Compliance Stakeholders	03.01.04.b	Separation of Duties	Define system access authorizations to support separation of duties.
N/A	N/A	03.01.05	Least Privilege	N/A
13	Identity & Access Management (IAM)	03.01.05.a	Least Privilege	Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.
13	Identity & Access Management (IAM)	03.01.05.b	Least Privilege	Authorize access to [Assignment: organization-defined security functions] and [Assignment: organization-defined security-relevant information].
13	Identity & Access Management (IAM)	03.01.05.c	Least Privilege	Review the privileges assigned to roles or classes of users [Assignment: organization-defined frequency] to validate the need for such privileges.
13	Identity & Access Management (IAM)	03.01.05.d	Least Privilege	Reassign or remove privileges, as necessary.
N/A	N/A	03.01.06	Least Privilege – Privileged Accounts	N/A
13	Identity & Access Management (IAM)	03.01.06.a	Least Privilege – Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]..
13	Identity & Access Management (IAM)	03.01.06.b	Least Privilege – Privileged Accounts	Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.
N/A	N/A	03.01.07	Least Privilege – Privileged Functions	N/A
13	Identity & Access Management (IAM)	03.01.07.a	Least Privilege – Privileged Functions	Prevent non-privileged users from executing privileged functions.
13	Identity & Access Management (IAM)	03.01.07.b	Least Privilege – Privileged Functions	Log the execution of privileged functions.
N/A	N/A	03.01.08	Unsuccessful Logon Attempts	N/A
12	Secure Baseline Configurations (SBC)	03.01.08.a	Unsuccessful Logon Attempts	Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period].
12	Secure Baseline Configurations (SBC)	03.01.08.b	Unsuccessful Logon Attempts	Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action] when the maximum number of unsuccessful attempts is exceeded.
12	Secure Baseline Configurations (SBC)	03.01.09	System Use Notification	Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.
N/A	N/A	03.01.10	Device Lock	N/A

12	Secure Baseline Configurations (SBC)	03.01.10.a	Device Lock	Prevent access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended].
12	Secure Baseline Configurations (SBC)	03.01.10.b	Device Lock	Retain the device lock until the user reestablishes access using established identification and authentication procedures.
12	Secure Baseline Configurations (SBC)	03.01.10.c	Device Lock	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.
12	Secure Baseline Configurations (SBC)	03.01.11	Session Termination	Terminate a user session automatically after [Assignment: organization-defined conditions or trigger events requiring session disconnect].
N/A	N/A	03.01.12	Remote Access	N/A
17	Layered Network Defenses	03.01.12.a	Remote Access	Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.
17	Layered Network Defenses	03.01.12.b	Remote Access	Authorize each type of remote system access prior to establishing such connections.
17	Layered Network Defenses	03.01.12.c	Remote Access	Route remote access to the system through authorized and managed access control points.
17	Layered Network Defenses	03.01.12.d	Remote Access	Authorize the remote execution of privileged commands and remote access to security-relevant information.
N/A	N/A	03.01.13	Withdrawn	Addressed by 03.13.08.
N/A	N/A	03.01.14	Withdrawn	Incorporated into 03.01.12.
N/A	N/A	03.01.15	Withdrawn	Incorporated into 03.01.12.
N/A	N/A	03.01.16	Wireless Access	N/A
17	Layered Network Defenses	03.01.16.a	Wireless Access	Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.
17	Layered Network Defenses	03.01.16.b	Wireless Access	Authorize each type of wireless access to the system prior to establishing such connections.
17	Layered Network Defenses	03.01.16.c	Wireless Access	Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.
17	Layered Network Defenses	03.01.16.d	Wireless Access	Protect wireless access to the system using authentication and encryption.
N/A	N/A	03.01.17	Withdrawn	Incorporated into 03.01.16.
N/A	N/A	03.01.18	Access Control for Mobile Devices	N/A
17	Layered Network Defenses	03.01.18.a	Access Control for Mobile Devices	Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.
17	Layered Network Defenses	03.01.18.b	Access Control for Mobile Devices	Authorize the connection of mobile devices to the system.
17	Layered Network Defenses	03.01.18.c	Access Control for Mobile Devices	Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.
N/A	N/A	03.01.19	Withdrawn	Incorporated into 03.01.18.
N/A	N/A	03.01.20	Use of External Systems	N/A
16	IT Asset Management (ITAM)	03.01.20.a	Use of External Systems	Prohibit the use of external systems unless the systems are specifically authorized.

16	IT Asset Management (ITAM)	03.01.20.b	Use of External Systems	Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [Assignment: organization-defined security requirements].
16	IT Asset Management (ITAM)	03.01.20.c	Use of External Systems	Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:
16	IT Asset Management (ITAM)	03.01.20.c.01	Use of External Systems	Verifying that the security requirements on the external systems as specified in the organization’s system security plans have been satisfied and
16	IT Asset Management (ITAM)	03.01.20.c.02	Use of External Systems	Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.
16	IT Asset Management (ITAM)	03.01.20.d	Use of External Systems	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.
N/A	N/A	03.01.21	Withdrawn	Incorporated into 03.01.20.
N/A	N/A	03.01.22	Publicly Accessible Content	N/A
6c	Identify Compliance Stakeholders	03.01.22.a	Publicly Accessible Content	Train authorized individuals to ensure that publicly accessible information does not contain CUI.
8	Segmented Network Architecture	03.01.22.b	Publicly Accessible Content	Review the content on publicly accessible systems for CUI and remove such information, if discovered.
N/A	N/A	03.02.01	Literacy Training and Awareness	N/A
21	Security Awareness Training	03.02.01.a	Literacy Training and Awareness	Provide security literacy training to system users:
21	Security Awareness Training	03.02.01.a.01	Literacy Training and Awareness	As part of initial training for new users and [Assignment: organization-defined frequency] thereafter,
21	Security Awareness Training	03.02.01.a.02	Literacy Training and Awareness	When required by system changes or following [Assignment: organization-defined events], and
21	Security Awareness Training	03.02.01.a.03	Literacy Training and Awareness	On recognizing and reporting indicators of insider threat, social engineering, and social mining.
21	Security Awareness Training	03.02.01.b	Literacy Training and Awareness	Update security literacy training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
N/A	N/A	03.02.02	Role-Based Training	N/A
21	Security Awareness Training	03.02.02.a	Role-Based Training	Provide role-based security training to organizational personnel:
21	Security Awareness Training	03.02.02.a.01	Role-Based Training	Before authorizing access to the system or CUI, before performing assigned duties, and [Assignment: organization-defined frequency] thereafter
21	Security Awareness Training	03.02.02.a.02	Role-Based Training	When required by system changes or following [Assignment: organization-defined events].
21	Security Awareness Training	03.02.02.b	Role-Based Training	Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
N/A	N/A	03.02.03	Withdrawn	Incorporated into 03.02.01.
N/A	N/A	03.03.01	Event Logging	N/A

11	Situational Awareness (SA)	03.03.01.a	Event Logging	Specify the following event types selected for logging within the system: [Assignment: organization-defined event types].
11	Situational Awareness (SA)	03.03.01.b	Event Logging	Review and update the event types selected for logging [Assignment: organization-defined frequency].
N/A	N/A	03.03.02	Audit Record Content	N/A
11	Situational Awareness (SA)	03.03.02.a	Audit Record Content	Include the following content in audit records:
11	Situational Awareness (SA)	03.03.02.a.01	Audit Record Content	What type of event occurred
11	Situational Awareness (SA)	03.03.02.a.02	Audit Record Content	When the event occurred
11	Situational Awareness (SA)	03.03.02.a.03	Audit Record Content	Where the event occurred
11	Situational Awareness (SA)	03.03.02.a.04	Audit Record Content	Source of the event
11	Situational Awareness (SA)	03.03.02.a.05	Audit Record Content	Outcome of the event
11	Situational Awareness (SA)	03.03.02.a.06	Audit Record Content	Identity of the individuals, subjects, objects, or entities associated with the event
11	Situational Awareness (SA)	03.03.02.b	Audit Record Content	Provide additional information for audit records as needed.
N/A	N/A	03.03.03	Audit Record Generation	N/A
11	Situational Awareness (SA)	03.03.03.a	Audit Record Generation	Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.
11	Situational Awareness (SA)	03.03.03.b	Audit Record Generation	Retain audit records for a time period consistent with the records retention policy.
N/A	N/A	03.03.04	Response to Audit Logging Process Failures	N/A
11	Situational Awareness (SA)	03.03.04.a	Response to Audit Logging Process Failures	Alert organizational personnel or roles within [Assignment: organization-defined time period] in the event of an audit logging process failure.
11	Situational Awareness (SA)	03.03.04.b	Response to Audit Logging Process Failures	Take the following additional actions: [Assignment: organization-defined additional actions].
N/A	N/A	03.03.05	Audit Record Review, Analysis, and Reporting	N/A
11	Situational Awareness (SA)	03.03.05.a	Audit Record Review, Analysis, and Reporting	Review and analyze system audit records [Assignment: organization-defined frequency] for indications and the potential impact of inappropriate or unusual activity.
11	Situational Awareness (SA)	03.03.05.b	Audit Record Review, Analysis, and Reporting	Report findings to organizational personnel or roles.
11	Situational Awareness (SA)	03.03.05.c	Audit Record Review, Analysis, and Reporting	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
N/A	N/A	03.03.06	Audit Record Reduction and Report Generation	N/A

11	Situational Awareness (SA)	03.03.06.a	Audit Record Reduction and Report Generation	Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.
11	Situational Awareness (SA)	03.03.06.b	Audit Record Reduction and Report Generation	Preserve the original content and time ordering of audit records.
N/A	N/A	03.03.07	Time Stamps	N/A
11	Situational Awareness (SA)	03.03.07.a	Time Stamps	Use internal system clocks to generate time stamps for audit records.
11	Situational Awareness (SA)	03.03.07.b	Time Stamps	Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.
N/A	N/A	03.03.08	Protection of Audit Information	N/A
11	Situational Awareness (SA)	03.03.08.a	Protection of Audit Information	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.
11	Situational Awareness (SA)	03.03.08.b	Protection of Audit Information	Authorize access to management of audit logging functionality to only a subset of privileged users or roles.
N/A	N/A	03.03.09	Withdrawn	Incorporated into 03.03.08.
N/A	N/A	03.04.01	Baseline Configuration	N/A
12	Secure Baseline Configurations (SBC)	03.04.01.a	Baseline Configuration	Develop and maintain under configuration control, a current baseline configuration of the system.
12	Secure Baseline Configurations (SBC)	03.04.01.b	Baseline Configuration	Review and update the baseline configuration of the system [Assignment: organization-defined frequency] and when system components are installed or modified.
N/A	N/A	03.04.02	Configuration Settings	N/A
12	Secure Baseline Configurations (SBC)	03.04.02.a	Configuration Settings	Establish, document, and implement the following configuration settings for the system that reflect the most restrictive mode consistent with operational requirements: [Assignment: organization-defined configuration settings].
12	Secure Baseline Configurations (SBC)	03.04.02.b	Configuration Settings	Identify, document, and approve any deviations from established configuration settings.
N/A	N/A	03.04.03	Configuration Change Control	N/A
7	Data Protection Practices	03.04.03.a	Configuration Change Control	Define the types of changes to the system that are configuration-controlled.
7	Data Protection Practices	03.04.03.b	Configuration Change Control	Review proposed configuration-controlled changes to the system, and approve or disapprove such changes with explicit consideration for security impacts.
7	Data Protection Practices	03.04.03.c	Configuration Change Control	Implement and document approved configuration-controlled changes to the system.
7	Data Protection Practices	03.04.03.d	Configuration Change Control	Monitor and review activities associated with configuration-controlled changes to the system.
N/A	N/A	03.04.04	Impact Analyses	N/A
7	Data Protection Practices	03.04.04.a	Impact Analyses	Analyze changes to the system to determine potential security impacts prior to change implementation.

7	Data Protection Practices	03.04.04.b	Impact Analyses	Verify that the security requirements for the system continue to be satisfied after the system changes have been implemented.
7	Data Protection Practices	03.04.05	Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
N/A	N/A	03.04.06	Least Functionality	N/A
12	Secure Baseline Configurations (SBC)	03.04.06.a	Least Functionality	Configure the system to provide only mission-essential capabilities.
12	Secure Baseline Configurations (SBC)	03.04.06.b	Least Functionality	Prohibit or restrict use of the following functions, ports, protocols, connections, and services: [Assignment: organization-defined functions, ports, protocols, connections, and services].
12	Secure Baseline Configurations (SBC)	03.04.06.c	Least Functionality	Review the system [Assignment: organization-defined frequency] to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.
12	Secure Baseline Configurations (SBC)	03.04.06.d	Least Functionality	Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.
N/A	N/A	03.04.07	Withdrawn	Incorporated into 03.04.06 and 03.04.08.
N/A	N/A	03.04.08	Authorized Software – Allow by Exception	N/A
12	Secure Baseline Configurations (SBC)	03.04.08.a	Authorized Software – Allow by Exception	Identify software programs authorized to execute on the system.
12	Secure Baseline Configurations (SBC)	03.04.08.b	Authorized Software – Allow by Exception	Implement a deny-all, allow-by-exception policy for the execution of authorized software programs on the system.
12	Secure Baseline Configurations (SBC)	03.04.08.c	Authorized Software – Allow by Exception	Review and update the list of authorized software programs [Assignment: organization-defined frequency].
N/A	N/A	03.04.09	Withdrawn	Addressed by 03.01.05, 03.01.06, 03.01.07, 03.04.08, and 03.12.03.
N/A	N/A	03.04.10	System Component Inventory	N/A
3b	Establish Compliance Scope	03.04.10.a	System Component Inventory	Develop and document an inventory of system components.
3b	Establish Compliance Scope	03.04.10.b	System Component Inventory	Review and update the system component inventory [Assignment: organization-defined frequency].
3b	Establish Compliance Scope	03.04.10.c	System Component Inventory	Update the system component inventory as part of installations, removals, and system updates.
N/A	N/A	03.04.11	Information Location	N/A
3c	Establish Compliance Scope	03.04.11.a	Information Location	Identify and document the location of CUI and the system components on which the information is processed and stored.
8	Segmented Network Architecture	03.04.11.b	Information Location	Document changes to the system or system component location where CUI is processed and stored.

N/A	N/A	03.04.12	System and Component Configuration for High-Risk Areas	N/A
12	Secure Baseline Configurations (SBC)	03.04.12.a	System and Component Configuration for High-Risk Areas	Issue systems or system components with the following configurations to individuals traveling to high-risk locations: [Assignment: organization-defined system configurations].
12	Secure Baseline Configurations (SBC)	03.04.12.b	System and Component Configuration for High-Risk Areas	Apply the following security requirements to the systems or components when the individuals return from travel: [Assignment: organization-defined security requirements].
N/A	N/A	03.05.01	User Identification and Authentication	N/A
13	Identity & Access Management (IAM)	03.05.01.a	User Identification and Authentication	Uniquely identify and authenticate system users, and associate that unique identification with processes acting on behalf of those users.
13	Identity & Access Management (IAM)	03.05.01.b	User Identification and Authentication	Re-authenticate users when [Assignment: organization-defined circumstances or situations requiring re-authentication].
13	Identity & Access Management (IAM)	03.05.02	Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices or types of devices] before establishing a system connection.
13	Identity & Access Management (IAM)	03.05.03	Multi-Factor Authentication	Implement multi-factor authentication for access to privileged and non-privileged accounts.
12	Secure Baseline Configurations (SBC)	03.05.04	Replay-Resistant Authentication	Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.
N/A	N/A	03.05.05	Identifier Management	N/A
13	Identity & Access Management (IAM)	03.05.05.a	Identifier Management	Receive authorization from organizational personnel or roles to assign an individual, group, role, service, or device identifier.
13	Identity & Access Management (IAM)	03.05.05.b	Identifier Management	Select and assign an identifier that identifies an individual, group, role, service, or device.
13	Identity & Access Management (IAM)	03.05.05.c	Identifier Management	Prevent the reuse of identifiers for [Assignment: organization-defined time period].
13	Identity & Access Management (IAM)	03.05.05.d	Identifier Management	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].
N/A	N/A	03.05.06	Identifier Management	Consistency with SP 800-53.
N/A	N/A	03.05.07	Password Management	N/A
13	Identity & Access Management (IAM)	03.05.07.a	Password Management	Maintain a list of commonly-used, expected, or compromised passwords, and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised.
13	Identity & Access Management (IAM)	03.05.07.b	Password Management	Verify that passwords are not found on the list of commonly used, expected, or compromised passwords when users create or update passwords.
12	Secure Baseline Configurations (SBC)	03.05.07.c	Password Management	Transmit passwords only over cryptographically protected channels.

12	Secure Baseline Configurations (SBC)	03.05.07.d	Password Management	Store passwords in a cryptographically protected form.
12	Secure Baseline Configurations (SBC)	03.05.07.e	Password Management	Select a new password upon first use after account recovery.
12	Secure Baseline Configurations (SBC)	03.05.07.f	Password Management	Enforce the following composition and complexity rules for passwords: [Assignment: organization-defined composition and complexity rules].
N/A	N/A	03.05.08	Password Management	Consistency with SP 800-53.
N/A	N/A	03.05.09	Password Management	Consistency with SP 800-53.
N/A	N/A	03.05.10	Withdrawn	Incorporated into 03.05.07.
12	Secure Baseline Configurations (SBC)	03.05.11	Authentication Feedback	Obscure feedback of authentication information during the authentication process.
N/A	N/A	03.05.12	Authenticator Management	N/A
13	Identity & Access Management (IAM)	03.05.12.a	Authenticator Management	Verify the identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution.
13	Identity & Access Management (IAM)	03.05.12.b	Authenticator Management	Establish initial authenticator content for any authenticators issued by the organization.
13	Identity & Access Management (IAM)	03.05.12.c	Authenticator Management	Establish and implement administrative procedures for initial authenticator distribution; for lost, compromised, or damaged authenticators; and for revoking authenticators.
13	Identity & Access Management (IAM)	03.05.12.d	Authenticator Management	Change default authenticators at first use.
13	Identity & Access Management (IAM)	03.05.12.e	Authenticator Management	Change or refresh authenticators [Assignment: organization-defined frequency] or when the following events occur: [Assignment: organization-defined events].
13	Identity & Access Management (IAM)	03.05.12.f	Authenticator Management	Protect authenticator content from unauthorized disclosure and modification.
10	Incident Response (IR)	03.06.01	Incident Handling	Implement an incident-handling capability that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.
N/A	N/A	03.06.02	Incident Monitoring, Reporting, and Response Assistance	N/A
10	Incident Response (IR)	03.06.02.a	Incident Monitoring, Reporting, and Response Assistance	Track and document system security incidents.
10	Incident Response (IR)	03.06.02.b	Incident Monitoring, Reporting, and Response Assistance	Report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period].

10	Incident Response (IR)	03.06.02.c	Incident Monitoring, Reporting, and Response Assistance	Report incident information to [Assignment: organization-defined authorities].
10	Incident Response (IR)	03.06.02.d	Incident Monitoring, Reporting, and Response Assistance	Provide an incident response support resource that offers advice and assistance to system users on handling and reporting incidents.
10	Incident Response (IR)	03.06.03	Incident Response Testing	Test the effectiveness of the incident response capability [Assignment: organization-defined frequency].
N/A	N/A	03.06.04	Incident Response Training	N/A
10	Incident Response (IR)	03.06.04.a	Incident Response Training	Provide incident response training to system users consistent with assigned roles and responsibilities:
10	Incident Response (IR)	03.06.04.a.01	Incident Response Training	Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access,
10	Incident Response (IR)	03.06.04.a.02	Incident Response Training	When required by system changes, and
10	Incident Response (IR)	03.06.04.a.03	Incident Response Training	[Assignment: organization-defined frequency] thereafter.
10	Incident Response (IR)	03.06.04.b	Incident Response Training	Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
N/A	N/A	03.06.05	Incident Response Plan	N/A
10	Incident Response (IR)	03.06.05.a	Incident Response Plan	Develop an incident response plan that:
10	Incident Response (IR)	03.06.05.a.01	Incident Response Plan	Provides the organization with a roadmap for implementing its incident response capability,
10	Incident Response (IR)	03.06.05.a.02	Incident Response Plan	Describes the structure and organization of the incident response capability,
10	Incident Response (IR)	03.06.05.a.03	Incident Response Plan	Provides a high-level approach for how the incident response capability fits into the overall organization,
10	Incident Response (IR)	03.06.05.a.04	Incident Response Plan	Defines reportable incidents,
10	Incident Response (IR)	03.06.05.a.05	Incident Response Plan	Addresses the sharing of incident information, and
10	Incident Response (IR)	03.06.05.a.06	Incident Response Plan	Designates responsibilities to organizational entities, personnel, or roles.
10	Incident Response (IR)	03.06.05.b	Incident Response Plan	Distribute copies of the incident response plan to designated incident response personnel (identified by name and/or by role) and organizational elements.
10	Incident Response (IR)	03.06.05.c	Incident Response Plan	Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing.
10	Incident Response (IR)	03.06.05.d	Incident Response Plan	Protect the incident response plan from unauthorized disclosure.
N/A	N/A	03.07.01	Withdrawn	Recategorized as NCO.
N/A	N/A	03.07.02	Withdrawn	Incorporated into 03.07.04 and 03.07.06.
N/A	N/A	03.07.03	Withdrawn	Incorporated into 03.08.03.

N/A	N/A	03.07.04	Maintenance Tools	N/A
14	Proactive Maintenance	03.07.04.a	Maintenance Tools	Approve, control, and monitor the use of system maintenance tools.
14	Proactive Maintenance	03.07.04.b	Maintenance Tools	Check media with diagnostic and test programs for malicious code before it is used in the system.
14	Proactive Maintenance	03.07.04.c	Maintenance Tools	Prevent the removal of system maintenance equipment containing CUI by verifying that there is no CUI on the equipment, sanitizing or destroying the equipment, or retaining the equipment within the facility.
N/A	N/A	03.07.05	Nonlocal Maintenance	N/A
14	Proactive Maintenance	03.07.05.a	Nonlocal Maintenance	Approve and monitor nonlocal maintenance and diagnostic activities.
14	Proactive Maintenance	03.07.05.b	Nonlocal Maintenance	Implement multi-factor authentication and replay resistance in the establishment of nonlocal maintenance and diagnostic sessions.
14	Proactive Maintenance	03.07.05.c	Nonlocal Maintenance	Terminate session and network connections when nonlocal maintenance is completed.
N/A	N/A	03.07.06	Maintenance Personnel	N/A
14	Proactive Maintenance	03.07.06.a	Maintenance Personnel	Establish a process for maintenance personnel authorization.
14	Proactive Maintenance	03.07.06.b	Maintenance Personnel	Maintain a list of authorized maintenance organizations or personnel.
14	Proactive Maintenance	03.07.06.c	Maintenance Personnel	Verify that non-escorted personnel who perform maintenance on the system possess the required access authorizations.
14	Proactive Maintenance	03.07.06.d	Maintenance Personnel	Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
8	Segmented Network Architecture	03.08.01	Media Storage	Physically control and securely store system media that contain CUI.
8	Segmented Network Architecture	03.08.02	Media Access	Restrict access to CUI on system media to authorized personnel or roles.
8	Segmented Network Architecture	03.08.03	Media Sanitization	Sanitize system media that contain CUI prior to disposal, release out of organizational control, or release for reuse.
8	Segmented Network Architecture	03.08.04	Media Marking	Mark system media that contain CUI to indicate distribution limitations, handling caveats, and applicable CUI markings.
N/A	N/A	03.08.05	Media Transport	N/A
8	Segmented Network Architecture	03.08.05.a	Media Transport	Protect and control system media that contain CUI during transport outside of controlled areas.
8	Segmented Network Architecture	03.08.05.b	Media Transport	Maintain accountability of system media that contain CUI during transport outside of controlled areas.
8	Segmented Network Architecture	03.08.05.c	Media Transport	Document activities associated with the transport of system media that contain CUI.
N/A	N/A	03.08.06	Withdrawn	Incorporated into 03.13.08.

N/A	N/A	03.08.07	Media Use	N/A
8	Segmented Network Architecture	03.08.07.a	Media Use	Restrict or prohibit the use of [Assignment: organization-defined types of system media].
8	Segmented Network Architecture	03.08.07.b	Media Use	Prohibit the use of removable system media without an identifiable owner.
N/A	N/A	03.08.08	Withdrawn	Incorporated into 03.08.07.
N/A	N/A	03.08.09	System Backup – Cryptographic Protection	N/A
18	Business Continuity / Disaster Recovery (BC/DR)	03.08.09.a	System Backup – Cryptographic Protection	Protect the confidentiality of backup information.
18	Business Continuity / Disaster Recovery (BC/DR)	03.08.09.b	System Backup – Cryptographic Protection	Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI at backup storage locations.
N/A	N/A	03.09.01	Personnel Screening	N/A
6b	Identify Compliance Stakeholders	03.09.01.a	Personnel Screening	Screen individuals prior to authorizing access to the system.
6b	Identify Compliance Stakeholders	03.09.01.b	Personnel Screening	Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening].
N/A	N/A	03.09.02	Personnel Termination and Transfer	N/A
6b	Identify Compliance Stakeholders	03.09.02.a	Personnel Termination and Transfer	When individual employment is terminated:
6b	Identify Compliance Stakeholders	03.09.02.a.01	Personnel Termination and Transfer	Disable system access within [Assignment: organization-defined time period],
6b	Identify Compliance Stakeholders	03.09.02.a.02	Personnel Termination and Transfer	Terminate or revoke authenticators and credentials associated with the individual, and
6b	Identify Compliance Stakeholders	03.09.02.a.03	Personnel Termination and Transfer	Retrieve security-related system property.
6b	Identify Compliance Stakeholders	03.09.02.b	Personnel Termination and Transfer	When individuals are reassigned or transferred to other positions in the organization:
6b	Identify Compliance Stakeholders	03.09.02.b.01	Personnel Termination and Transfer	Review and confirm the ongoing operational need for current logical and physical access authorizations to the system and facility, and
6b	Identify Compliance Stakeholders	03.09.02.b.02	Personnel Termination and Transfer	Modify access authorization to correspond with any changes in operational need.
N/A	N/A	03.10.01	Physical Access Authorizations	N/A
20	Physical Security	03.10.01.a	Physical Access Authorizations	Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.
20	Physical Security	03.10.01.b	Physical Access Authorizations	Issue authorization credentials for facility access.

20	Physical Security	03.10.01.c	Physical Access Authorizations	Review the facility access list [Assignment: organization-defined frequency].
20	Physical Security	03.10.01.d	Physical Access Authorizations	Remove individuals from the facility access list when access is no longer required.
N/A	N/A	03.10.02	Monitoring Physical Access	N/A
20	Physical Security	03.10.02.a	Monitoring Physical Access	Monitor physical access to the facility where the system resides to detect and respond to physical security incidents.
20	Physical Security	03.10.02.b	Monitoring Physical Access	Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indicators of events].
N/A	N/A	03.10.03	Withdrawn	Incorporated into 03.10.07.
N/A	N/A	03.10.04	Withdrawn	Incorporated into 03.10.07.
N/A	N/A	03.10.05	Withdrawn	Incorporated into 03.10.07.
N/A	N/A	03.10.06	Alternate Work Site	N/A
20	Physical Security	03.10.06.a	Alternate Work Site	Determine alternate work sites allowed for use by employees.
20	Physical Security	03.10.06.b	Alternate Work Site	Employ the following security requirements at alternate work sites: [Assignment: organization-defined security requirements].
N/A	N/A	03.10.07	Physical Access Control	N/A
20	Physical Security	03.10.07.a	Physical Access Control	Enforce physical access authorizations at entry and exit points to the facility where the system resides by:
20	Physical Security	03.10.07.a.01	Physical Access Control	Verifying individual physical access authorizations before granting access to the facility and
20	Physical Security	03.10.07.a.02	Physical Access Control	Controlling ingress and egress with physical access control systems, devices, or guards.
20	Physical Security	03.10.07.b	Physical Access Control	Maintain physical access audit logs for entry or exit points.
20	Physical Security	03.10.07.c	Physical Access Control	Escort visitors, and control visitor activity.
20	Physical Security	03.10.07.d	Physical Access Control	Secure keys, combinations, and other physical access devices.
20	Physical Security	03.10.07.e	Physical Access Control	Control physical access to output devices to prevent unauthorized individuals from obtaining access to CUI.
20	Physical Security	03.10.08	Access Control for Transmission	Control physical access to system distribution and transmission lines within organizational facilities.
N/A	N/A	03.11.01	Risk Assessment	N/A
4a	Risk Management Practices	03.11.01.a	Risk Assessment	Assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI.
4a	Risk Management Practices	03.11.01.b	Risk Assessment	Update risk assessments [Assignment: organization-defined frequency].
N/A	N/A	03.11.02	Vulnerability Monitoring and Scanning	N/A
15	Attack Surface Management (ASM)	03.11.02.a	Vulnerability Monitoring and Scanning	Monitor and scan the system for vulnerabilities [Assignment: organization-defined frequency] and when new vulnerabilities affecting the system are identified.

15	Attack Surface Management (ASM)	03.11.02.b	Vulnerability Monitoring and Scanning	Remediate system vulnerabilities within [Assignment: organization-defined response times].
15	Attack Surface Management (ASM)	03.11.02.c	Vulnerability Monitoring and Scanning	Update system vulnerabilities to be scanned [Assignment: organization-defined frequency] and when new vulnerabilities are identified and reported.
N/A	N/A	03.11.03	Withdrawn	Incorporated into 03.11.02.
4a	Risk Management Practices	03.11.04	Risk Response	Respond to findings from security assessments, monitoring, and audits.
22	Internal Audit (IA)	03.12.01	Security Assessment	Assess the security requirements for the system and its environment of operation [Assignment: organization-defined frequency] to determine if the requirements have been satisfied.
N/A	N/A	03.12.02	Plan of Action and Milestones	N/A
5b	Document The CUI and/or FCI Environment	03.12.02.a	Plan of Action and Milestones	Develop a plan of action and milestones for the system:
5b	Document The CUI and/or FCI Environment	03.12.02.a.01	Plan of Action and Milestones	To document the planned remediation actions to correct weaknesses or deficiencies noted during security assessments and
5b	Document The CUI and/or FCI Environment	03.12.02.a.02	Plan of Action and Milestones	To reduce or eliminate known system vulnerabilities.
5b	Document The CUI and/or FCI Environment	03.12.02.b	Plan of Action and Milestones	Update the existing plan of action and milestones based on the findings from:
5b	Document The CUI and/or FCI Environment	03.12.02.b.01	Plan of Action and Milestones	Security assessments,
5b	Document The CUI and/or FCI Environment	03.12.02.b.02	Plan of Action and Milestones	Audits or reviews, and
5b	Document The CUI and/or FCI Environment	03.12.02.b.03	Plan of Action and Milestones	Continuous monitoring activities.
11	Situational Awareness (SA)	03.12.03	Continuous Monitoring	Develop and implement a system-level continuous monitoring strategy that includes ongoing monitoring and security assessments.
N/A	N/A	03.12.04	Withdrawn	Incorporated into 03.15.02.
N/A	N/A	03.12.05	Information Exchange	N/A
8	Segmented Network Architecture	03.12.05.a	Information Exchange	Approve and manage the exchange of CUI between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service-level agreements; user agreements; non-disclosure agreements; other types of agreements].
8	Segmented Network Architecture	03.12.05.b	Information Exchange	Document interface characteristics, security requirements, and responsibilities for each system as part of the exchange agreements.
8	Segmented Network Architecture	03.12.05.c	Information Exchange	Review and update the exchange agreements [Assignment: organization-defined frequency].

N/A	N/A	03.13.01	Boundary Protection	N/A
9	Change Management (CM)	03.13.01.a	Boundary Protection	Monitor and control communications at external managed interfaces to the system and key internal managed interfaces within the system.
9	Change Management (CM)	03.13.01.b	Boundary Protection	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
9	Change Management (CM)	03.13.01.c	Boundary Protection	Connect to external systems only through managed interfaces that consist of boundary protection devices arranged in accordance with an organizational security architecture.
N/A	N/A	03.13.02	Boundary Protection	Recategorized as NCO.
N/A	N/A	03.13.03	Withdrawn	Addressed by 03.01.01, 03.01.02, 03.01.03, 03.01.04, 03.01.05, 03.01.06, and 03.01.07.
12	Secure Baseline Configurations (SBC)	03.13.04	Information in Shared System Resources	Prevent unauthorized and unintended information transfer via shared system resources.
N/A	N/A	03.13.05	Withdrawn	Incorporated into 03.13.01.
9	Change Management (CM)	03.13.06	Network Communications – Deny by Default – Allow by Exception	Deny network communications traffic by default, and allow network communications traffic by exception.
N/A	N/A	03.13.07	Withdrawn	Addressed by 03.01.12, 03.04.02 and 03.04.06.
19	Cryptographic Key Management	03.13.08	Transmission and Storage Confidentiality	Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.
12	Secure Baseline Configurations (SBC)	03.13.09	Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.
19	Cryptographic Key Management	03.13.10	Cryptographic Key Establishment and Management	Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].
19	Cryptographic Key Management	03.13.11	Cryptographic Protection	Implement the following types of cryptography to protect the confidentiality of CUI: [Assignment: organization-defined types of cryptography].
N/A	N/A	03.13.12	Collaborative Computing Devices and Applications	N/A
12	Secure Baseline Configurations (SBC)	03.13.12.a	Collaborative Computing Devices and Applications	Prohibit the remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed].
12	Secure Baseline Configurations (SBC)	03.13.12.b	Collaborative Computing Devices and Applications	Provide an explicit indication of use to users physically present at the devices.
N/A	N/A	03.13.13	Mobile Code	N/A

12	Secure Baseline Configurations (SBC)	03.13.13.a	Mobile Code	Define acceptable mobile code and mobile code technologies.
12	Secure Baseline Configurations (SBC)	03.13.13.b	Mobile Code	Authorize, monitor, and control the use of mobile code.
N/A	N/A	03.13.14	Withdrawn	Technology-specific.
19	Cryptographic Key Management	03.13.15	Session Authenticity	Protect the authenticity of communications sessions.
N/A	N/A	03.13.16	Withdrawn	Incorporated into 03.13.08.
N/A	N/A	03.14.01	Flaw Remediation	N/A
15	Attack Surface Management (ASM)	03.14.01.a	Flaw Remediation	Identify, report, and correct system flaws.
15	Attack Surface Management (ASM)	03.14.01.b	Flaw Remediation	Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates.
N/A	N/A	03.14.02	Malicious Code Protection	N/A
15	Attack Surface Management (ASM)	03.14.02.a	Malicious Code Protection	Implement malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.
15	Attack Surface Management (ASM)	03.14.02.b	Malicious Code Protection	Update malicious code protection mechanisms as new releases are available in accordance with configuration management policies and procedures.
15	Attack Surface Management (ASM)	03.14.02.c	Malicious Code Protection	Configure malicious code protection mechanisms to:
15	Attack Surface Management (ASM)	03.14.02.c.01	Malicious Code Protection	Perform scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoints or system entry and exit points as the files are downloaded, opened, or executed; and
15	Attack Surface Management (ASM)	03.14.02.c.02	Malicious Code Protection	Block malicious code, quarantine malicious code, or take other mitigation actions in response to malicious code detection.
N/A	N/A	03.14.03	Security Alerts, Advisories, and Directives	N/A
11	Situational Awareness (SA)	03.14.03.a	Security Alerts, Advisories, and Directives	Receive system security alerts, advisories, and directives from external organizations on an ongoing basis.
11	Situational Awareness (SA)	03.14.03.b	Security Alerts, Advisories, and Directives	Generate and disseminate internal system security alerts, advisories, and directives, as necessary.
N/A	N/A	03.14.04	Withdrawn	Incorporated into 03.14.02.
N/A	N/A	03.14.05	Withdrawn	Addressed by 03.14.02.
N/A	N/A	03.14.06	System Monitoring	N/A
11	Situational Awareness (SA)	03.14.06.a	System Monitoring	Monitor the system to detect:
11	Situational Awareness (SA)	03.14.06.a.01	System Monitoring	Attacks and indicators of potential attacks and
11	Situational Awareness (SA)	03.14.06.a.02	System Monitoring	Unauthorized connections.

11	Situational Awareness (SA)	03.14.06.b	System Monitoring	Identify unauthorized use of the system.
11	Situational Awareness (SA)	03.14.06.c	System Monitoring	Monitor inbound and outbound communications traffic to detect unusual or unauthorized activities or conditions.
N/A	N/A	03.14.07	Withdrawn	Incorporated into 03.14.06.
8	Segmented Network Architecture	03.14.08	Information Management and Retention	Manage and retain CUI within the system and CUI output from the system in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.
N/A	N/A	03.15.01	Policy and Procedures	N/A
2a	Implement Governance Practices	03.15.01.a	Policy and Procedures	Develop, document, and disseminate to organizational personnel or roles the policies and procedures needed to satisfy the security requirements for the protection of CUI.
2a	Implement Governance Practices	03.15.01.b	Policy and Procedures	Review and update policies and procedures [Assignment: organization-defined frequency].
N/A	N/A	03.15.02	System Security Plan	N/A
5a	Document The CUI and/or FCI Environment	03.15.02.a	System Security Plan	Develop a system security plan that:
5a	Document The CUI and/or FCI Environment	03.15.02.a.01	System Security Plan	Defines the constituent system components;
5a	Document The CUI and/or FCI Environment	03.15.02.a.02	System Security Plan	Identifies the information types processed, stored, and transmitted by the system;
5a	Document The CUI and/or FCI Environment	03.15.02.a.03	System Security Plan	Describes specific threats to the system that are of concern to the organization;
5a	Document The CUI and/or FCI Environment	03.15.02.a.04	System Security Plan	Describes the operational environment for the system and any dependencies on or connections to other systems or system components;
5a	Document The CUI and/or FCI Environment	03.15.02.a.05	System Security Plan	Provides an overview of the security requirements for the system;
5a	Document The CUI and/or FCI Environment	03.15.02.a.06	System Security Plan	Describes the safeguards in place or planned for meeting the security requirements;
5a	Document The CUI and/or FCI Environment	03.15.02.a.07	System Security Plan	Identifies individuals that fulfill system roles and responsibilities; and
5a	Document The CUI and/or FCI Environment	03.15.02.a.08	System Security Plan	Includes other relevant information necessary for the protection of CUI.
5a	Document The CUI and/or FCI Environment	03.15.02.b	System Security Plan	Review and update the system security plan [Assignment: organization-defined frequency].
5a	Document The CUI and/or FCI Environment	03.15.02.c	System Security Plan	Protect the system security plan from unauthorized disclosure.
N/A	N/A	03.15.03	Rules of Behavior	N/A

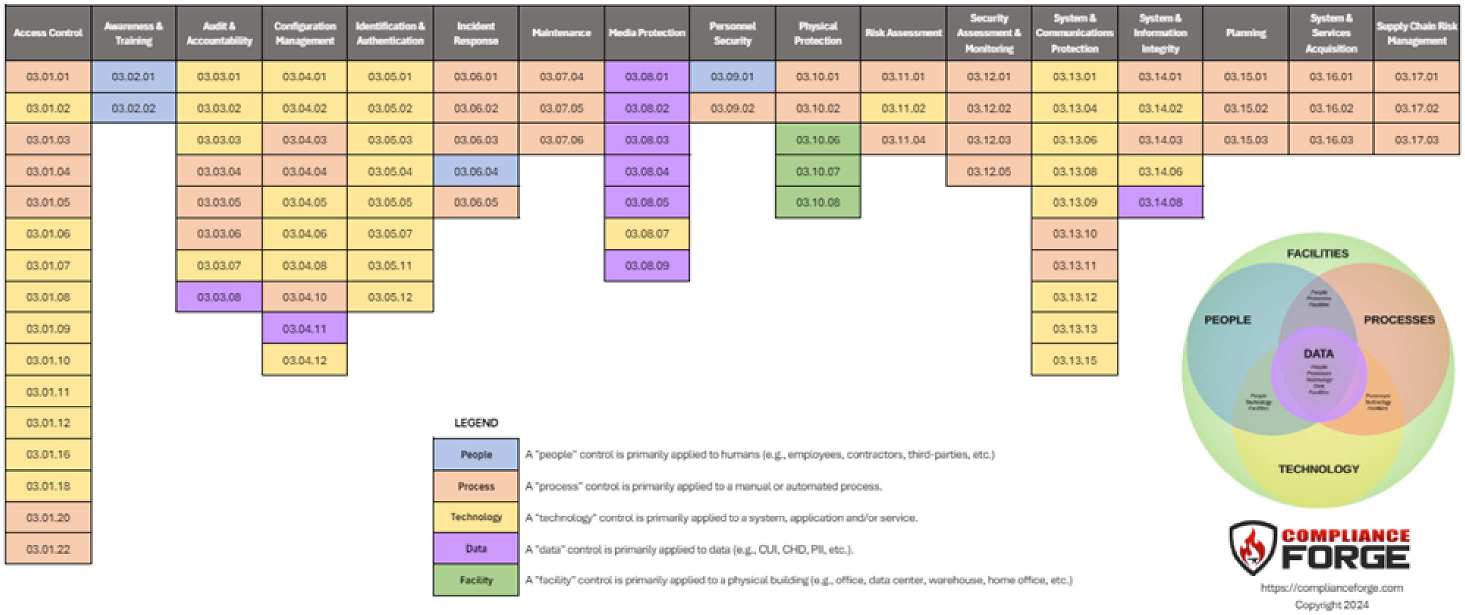
6b	Identify Compliance Stakeholders	03.15.03.a	Rules of Behavior	Establish rules that describe the responsibilities and expected behavior for system usage and protecting CUI.
6b	Identify Compliance Stakeholders	03.15.03.b	Rules of Behavior	Provide rules to individuals who require access to the system.
6b	Identify Compliance Stakeholders	03.15.03.c	Rules of Behavior	Receive a documented acknowledgement from individuals indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to CUI and the system.
6b	Identify Compliance Stakeholders	03.15.03.d	Rules of Behavior	Review and update the rules of behavior [Assignment: organization-defined frequency].
9	Change Management (CM)	03.16.01	Security Engineering Principles	Apply the following systems security engineering principles to the development or modification of the system and system components: [Assignment: organization-defined systems security engineering principles].
N/A	N/A	03.16.02	Unsupported System Components	N/A
16	IT Asset Management (ITAM)	03.16.02.a	Unsupported System Components	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer.
16	IT Asset Management (ITAM)	03.16.02.b	Unsupported System Components	Provide options for risk mitigation or alternative sources for continued support for unsupported components that cannot be replaced.
N/A	N/A	03.16.03	External System Services	N/A
4c	Risk Management Practices	03.16.03.a	External System Services	Require the providers of external system services used for the processing, storage, or transmission of CUI to comply with the following security requirements: [Assignment: organization-defined security requirements].
3e	Establish Compliance Scope	03.16.03.b	External System Services	Define and document user roles and responsibilities with regard to external system services, including shared responsibilities with external service providers.
4e	Risk Management Practices	03.16.03.c	External System Services	Implement processes, methods, and techniques to monitor security requirement compliance by external service providers on an ongoing basis.
N/A	N/A	03.17.01	Supply Chain Risk Management Plan	N/A
4b	Risk Management Practices	03.17.01.a	Supply Chain Risk Management Plan	Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of the system, system components, or system services.
4b	Risk Management Practices	03.17.01.b	Supply Chain Risk Management Plan	Review and update the supply chain risk management plan [Assignment: organization-defined frequency].
4b	Risk Management Practices	03.17.01.c	Supply Chain Risk Management Plan	Protect the supply chain risk management plan from unauthorized disclosure.
4c	Risk Management Practices	03.17.02	Acquisition Strategies, Tools, and Methods	Develop and implement acquisition strategies, contract tools, and procurement methods to identify, protect against, and mitigate supply chain risks.
N/A	N/A	03.17.03	Supply Chain Requirements and Processes	N/A

4e	Risk Management Practices	03.17.03.a	Supply Chain Requirements and Processes	Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.
4d	Risk Management Practices	03.17.03.b	Supply Chain Requirements and Processes	Enforce the following security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined security requirements].

APPENDIX A – UNDERSTANDING CONTROL APPLICABILITY

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

When you break down NIST 800-171 R3 requirements into how they are operationalized, the controls are applicable to people, processes, technology, data or facilities. This "NIST 800-171 R3 In A Nutshell" graphic can be downloaded from: https://content.complianceforge.com/graphics/nist-800-171-r3-nutshell.pdf



Access Control	Awareness & Training	Audit & Accountability	Configuration Management	Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Risk Assessment	Security Assessment & Monitoring	System & Communications Protection	System & Information Integrity	Planning	System & Services Acquisition	Supply Chain Risk Management
🟧 03.01.01	🟦 03.02.01	🟨 03.03.01	🟨 03.04.01	🟨 03.05.01	🟧 03.06.01	🟧 03.07.04	🟪 03.08.01	🟦 03.09.01	🟧 03.10.01	🟧 03.11.01	🟧 03.12.01	🟨 03.13.01	🟧 03.14.01	🟧 03.15.01	🟧 03.16.01	🟧 03.17.01
🟨 03.01.02	🟦 03.02.02	🟨 03.03.02	🟨 03.04.02	🟨 03.05.02	🟧 03.06.02	🟧 03.07.05	🟪 03.08.02	🟧 03.09.02	🟧 03.10.02	🟨 03.11.02	🟧 03.12.02	🟨 03.13.04	🟨 03.14.02	🟧 03.15.02	🟧 03.16.02	🟧 03.17.02
🟧 03.01.03		🟨 03.03.03	🟧 03.04.03	🟨 03.05.03	🟧 03.06.03	🟧 03.07.06	🟪 03.08.03		🟩 03.10.06	🟧 03.11.04	🟧 03.12.03	🟨 03.13.06	🟧 03.14.03	🟧 03.15.03	🟧 03.16.03	🟧 03.17.03
🟧 03.01.04		🟧 03.03.04	🟧 03.04.04	🟨 03.05.04	🟦 03.06.04		🟪 03.08.04		🟩 03.10.07		🟧 03.12.05	🟨 03.13.08	🟨 03.14.06			
🟧 03.01.05		🟧 03.03.05	🟨 03.04.05	🟨 03.05.05	🟧 03.06.05		🟪 03.08.05		🟩 03.10.08			🟨 03.13.09	🟪 03.14.08			
🟨 03.01.06		🟧 03.03.06	🟨 03.04.06	🟨 03.05.07			🟨 03.08.07					🟧 03.13.10				
🟨 03.01.07		🟨 03.03.07	🟨 03.04.08	🟨 03.05.11			🟪 03.08.09					🟧 03.13.11				
🟨 03.01.08		🟪 03.03.08	🟧 03.04.10	🟨 03.05.12								🟨 03.13.12				
🟨 03.01.09			🟪 03.04.11									🟨 03.13.13				
🟨 03.01.10			🟨 03.04.12									🟨 03.13.15				
🟨 03.01.11																
🟨 03.01.12																
🟨 03.01.16																
🟨 03.01.18																
🟧 03.01.20																
🟧 03.01.22																

LEGEND

🟦 People	A "people" control is primarily applied to humans (e.g., employees, contractors, third-parties, etc.)
🟧 Process	A "process" control is primarily applied to a manual or automated process.
🟨 Technology	A "technology" control is primarily applied to a system, application and/or service.
🟪 Data	A "data" control is primarily applied to data (e.g., CUI, CHD, PII, etc.).
🟩 Facility	A "facility" control is primarily applied to a physical building (e.g., office, data center, warehouse, home office, etc.)

https://complianceforge.com
Copyright 2024

Examples to help demonstrate the applicable nature of controls:

- You cannot apply end user training to a firewall (technology).
- An employee (people) cannot have a secure baseline configuration applied.
- An Incident Response Plan (IRP) (process) cannot sign a NDA, use MFA or be patched.
- Controlled Unclassified Information (CUI) (data) cannot be assigned roles and responsibilities.
- Your data center (facility) cannot undergo employee background screening.

The PPTDF model, encompassing People, Processes, Technology, Data, and Facilities, provides a comprehensive approach to cybersecurity control applicability, as described below:

PEOPLE

People are often considered the weakest link in cybersecurity. Human error, negligence, or malicious intent can lead to significant vulnerabilities. To mitigate these risks, organizations implement human-specific controls such as:

- Security Awareness Training: Educating employees about cybersecurity best practices and potential threats.
- Access Controls: Enforcing the principle of least privilege to restrict access based on job roles.
- User Authentication and Authorization: Implementing strong authentication mechanisms and carefully managing user permissions.

PROCESSES

Effective cybersecurity processes are essential for identifying, responding to, and mitigating threats. Common processes that exist as controls include:

- Incident Response Plans: Establishing well-defined processes to respond promptly and effectively to security incidents.
- Regular Audits and Assessments: Conducting periodic assessments to identify vulnerabilities and measure compliance with security policies.

- Change Management: Implementing controls to manage changes in technology and processes to avoid unintended security consequences.

TECHNOLOGY

The technological aspect of cybersecurity involves deploying and configuring tools to protect against threats. Common technologies that exist as controls include:

- Network Defenses: Filtering and monitoring network traffic to prevent unauthorized access (e.g., firewalls, Intrusion Protection Systems (IPS), Data Loss Prevention (DLP), etc.).
- Endpoint Protection: Installing antimalware software, Endpoint Detection and Response (EDR) tools to secure individual devices, etc.
- Encryption: Safeguarding data in transit and at rest through robust encryption mechanisms.

DATA

Data is at the heart of the PPTDF model, making data protection truly the central focus of cybersecurity controls. There are many types of data that are considered sensitive/regulated that include, but are not limited to:

- Controlled Unclassified Information (CUI),
- Federal Contract Information (FCI),
- Personally Identifiable Information (PII),
- Cardholder Data (CHD),
- Export-Controlled Data (ITAR / EAR),
- Electronic Protected Health Information (ePHI),
- Intellectual Property (IP),
- Critical Infrastructure Information (CII),
- Attorney-Client Privilege Information (ACPI) and
- Student Educational Records (FERPA).

These data types have specific controls that are dictated by applicable laws, regulations or contractual obligations and include:

- Data Classification: Data must be categorized to apply the appropriate security measures.
- Limited Access: Data must be protected by limiting logical and physical access to data to individuals and systems that have a legitimate business need.
- Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) Data: Data must be trustworthy, based on the data's currency, accuracy, integrity and/or applicability.
- Availability: Data must be available, which involves regularly backing up data and establishing effective data recovery mechanisms that protects the integrity and confidentiality of the data being backed up and recovered.

FACILITIES

Physical security is often overlooked but plays a crucial role in overall cybersecurity and data protection. Common physical controls include:

- Physical Access Control (PAC): Restricting physical access to any facility where systems or data exist. PAC exists in more than datacenters and corporate offices. The concept of PAC extends to home offices and Work From Anywhere (WFA) workers who still have an obligation to apply physical security protections to their systems and data.
- Surveillance Systems: Monitoring and recording activities within facilities to detect and deter unauthorized access.
- Environmental Controls: Maintaining optimal conditions for hardware to prevent damage or disruptions.

The PPTDF model shows that a multi-faceted approach to control applicability is indispensable, where it can create a resilient defense against a myriad of physical and cyber threats. A proactive stance in implementing and refining these controls will be crucial in securing the ever-expanding digital frontier.

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

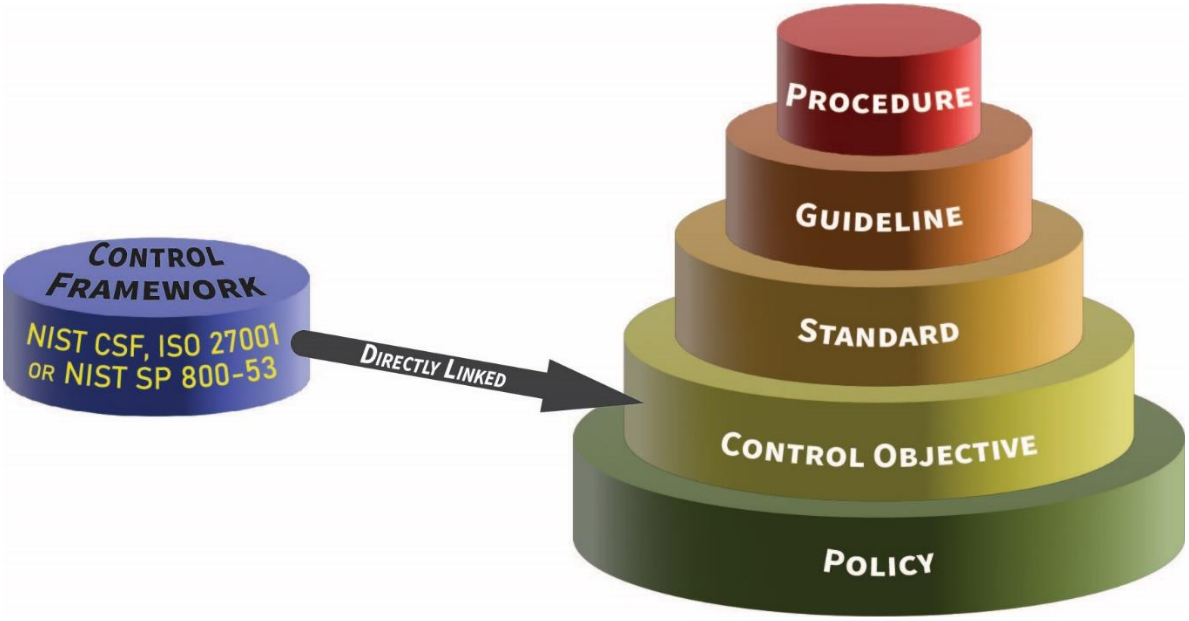
The purpose of a company's cybersecurity documentation is to prescribe a comprehensive framework for:

- 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 cybersecurity & data privacy documentation is comprised of six (6) core components:

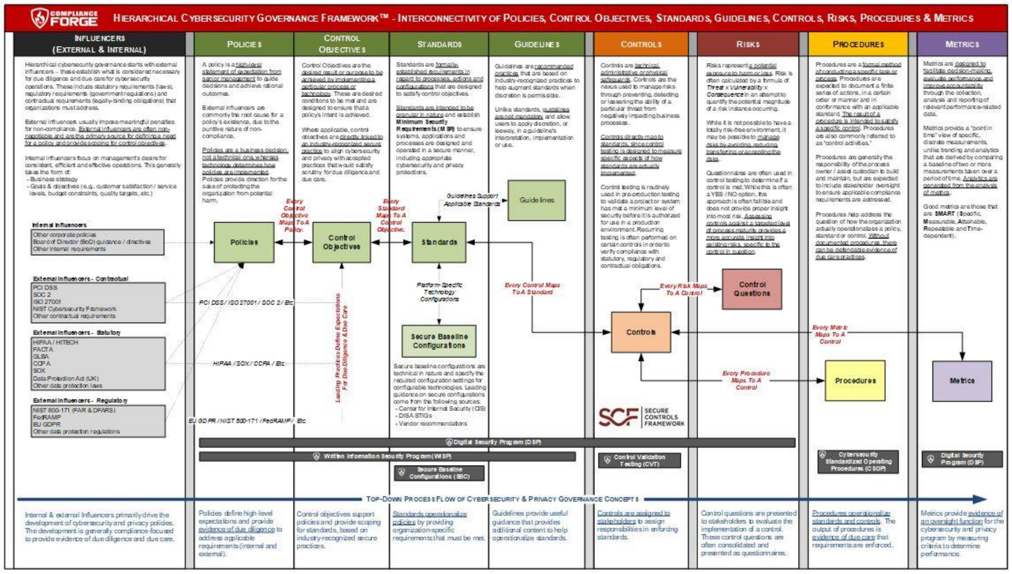
(1) Policies that establish management's intent;
(2) Control objective that identifies leading practices;
(3) Standards that provides quantifiable requirements;
(4) Controls identify desired conditions that are expected to be met;
(5) Procedures / Control Activities establish how tasks are performed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



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/grc/hierarchical-cybersecurity-governance-framework/


COMPLIANCE FORGE
Hierarchical Cybersecurity Governance Framework™ - Interconnectivity of Policies, Control Objectives, Standards, Guidelines, Controls, Risks, Procedures & Metrics
Influencers (External & Internal)
Policies
Control Objectives
Standards
Guidelines
Controls
Risks
Procedures
Metrics
Hierarchical cybersecurity governance starts with external influencers – these establish what is considered necessary for due diligence and due care for cybersecurity operations. These include statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding obligations) that organizations must address.
External influencers usually impose meaningful penalties for non-compliance. External influencers are often non-negotiable and are the primary source for defining a need for a policy and provide scoping for control objectives.
Internal influencers focus on management's desire for consistent, efficient and effective operations. This generally takes the form of:
- Business strategy
- Goals & objectives (e.g., customer satisfaction / service levels, budget constraints, quality targets, etc.)
A policy is a high-level statement of expectation from senior management to guide decisions and achieve rational outcomes.
External influencers are commonly the root cause for a policy's existence, due to the punitive nature of non-compliance.
Policies are a business decision, not a technical one whereas technology determines how policies are implemented. Policies provide direction for the sake of protecting the organization from potential harm.
Control Objectives are the desired result or purpose to be achieved by implementing a particular process or technology. These are desired conditions to be met and are designed to ensure that a policy's intent is achieved.
Where applicable, control objectives are directly linked to an industry-recognized secure practice to align cybersecurity and privacy with accepted practices that would satisfy scrutiny for due diligence and due care.
Standards are formally-established requirements in regard to processes, actions and configurations that are designed to satisfy control objectives.
Standards are intended to be granular in nature and establish Minimum Security Requirements (MSR) to ensure systems, applications and processes are designed and operated in a secure manner, including appropriate cybersecurity and privacy protections.
Guidelines are recommended practices that are based on industry-recognized practices to help augment standards when discretion is permissible.
Unlike standards, guidelines are not mandatory and allow users to apply discretion, or leeway, in a guideline's interpretation, implementation or use.
Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessering the ability of a particular threat from negatively impacting business processes.
Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.
Control testing is routinely used in pre-production testing to validate a project or system has met a minimum level of security before it is authorized for use in a production environment. Recurring testing is often performed on certain controls in order to verify compliance with statutory, regulatory and contractual obligations.
Risks represent a potential exposure to harm or loss. Risk is often calculated by a formula of Threat x Vulnerability x Consequence in an attempt to quantify the potential magnitude of a risk instance occurring.
While it is not possible to have a totally risk-free environment, it may be possible to manage risks by avoiding, reducing, transferring or accepting the risks.
Questionnaires are often used in control testing to determine if a control is met. While this is often a YES / NO option, this approach is often fallible and does not provide proper insight into most risk. Assessing controls against a targeted level of process maturity provides a more accurate insight into existing risks, specific to the control in question.
Procedures are a formal method of conducting a specific task or process. Procedures are expected to document a finite series of actions, in a certain order or manner and in conformance with an applicable standard. The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as "control activities."
Procedures are generally the responsibility of the process owner / asset custodian to build and maintain, but are expected to include stakeholder oversight to ensure applicable compliance requirements are addressed.
Procedures help address the question of how the organization actually operationalizes a policy, standard or control. Without documented procedures, there can be defendable evidence of due care practices.
Metrics are designed to facilitate decision-making, evaluate performance and improve accountability through the collection, analysis and reporting of relevant performance-related data.
Metrics provide a "point in time" view of specific, discrete measurements, unlike trending and analytics that are derived by comparing a baseline of two or more measurements taken over a period of time. Analytics are generated from the analysis of metrics.
Good metrics are those that are SMART (Specific, Measurable, Attainable, Repeatable and Time-dependent).
Internal Influencers
Other corporate policies
Board of Director (BoD) guidance / directives
Other internal requirements
External Influencers - Contractual
PCI DSS
SOC 2
ISO 27001
NIST Cybersecurity Framework
Other contractual requirements
External Influencers - Statutory
HIPAA / HITECH
FACTA
GLBA
CCPA
SOX
Data Protection Act (UK)
Other data protection laws
External Influencers - Regulatory
NIST 800-171 (FAR & DFARS)
FedRAMP
EU GDPR
Other data protection regulations
PCI DSS / ISO 27001 / SOC 2 / Etc
HIPAA / SOX / CCPA / Etc
EU GDPR / NIST 800-171 / FedRAMP / Etc
Policies
Every Control Objective Maps To A Policy.
Control Objectives
Every Standard Maps To A Control Objective.
Standards
Guidelines Support Applicable Standards
Guidelines
Leading Practices Define Expectations For Due Diligence & Due Care
Platform-Specific Technology Configurations
Secure Baseline Configurations
Secure baseline configurations are technical in nature and specify the required configuration settings for configurable technologies. Leading guidance on secure configurations come from the following sources:
- Center for Internet Security (CIS)
- DISA STIGs
- Vendor recommendations
Every Control Maps To A Standard
Controls
Every Risk Maps To A Control
Control Questions
Every Metric Maps To A Control
Every Procedure Maps To A Control
Procedures
Metrics
SCF SECURE CONTROLS FRAMEWORK
Digital Security Program (DSP)
Written Information Security Program (WISP)
Secure Baseline Configurations (SBC)
Control Validation Testing (CVT)
Cybersecurity Standardized Operating Procedures (CSOP)
Digital Security Program (DSP)
Top-Down Process Flow of Cybersecurity & Privacy Governance Concepts
Internal & external influencers primarily drive the development of cybersecurity and privacy policies. The development is generally compliance-focused to provide evidence of due diligence and due care.
Policies define high-level expectations and provide evidence of due diligence to address applicable requirements (internal and external).
Control objectives support policies and provide scoping for standards, based on industry-recognized secure practices.
Standards operationalize policies by providing organization-specific requirements that must be met.
Guidelines provide useful guidance that provides additional content to help operationalize standards.
Controls are assigned to stakeholders to assign responsibilities in enforcing standards.
Control questions are presented to stakeholders to evaluate the implementation of a control. These control questions are often consolidated and presented as questionnaires.
Procedures operationalize standards and controls. The output of procedures is evidence of due care that requirements are enforced.
Metrics provide evidence of an oversight function for the cybersecurity and privacy program by measuring criteria to determine performance.