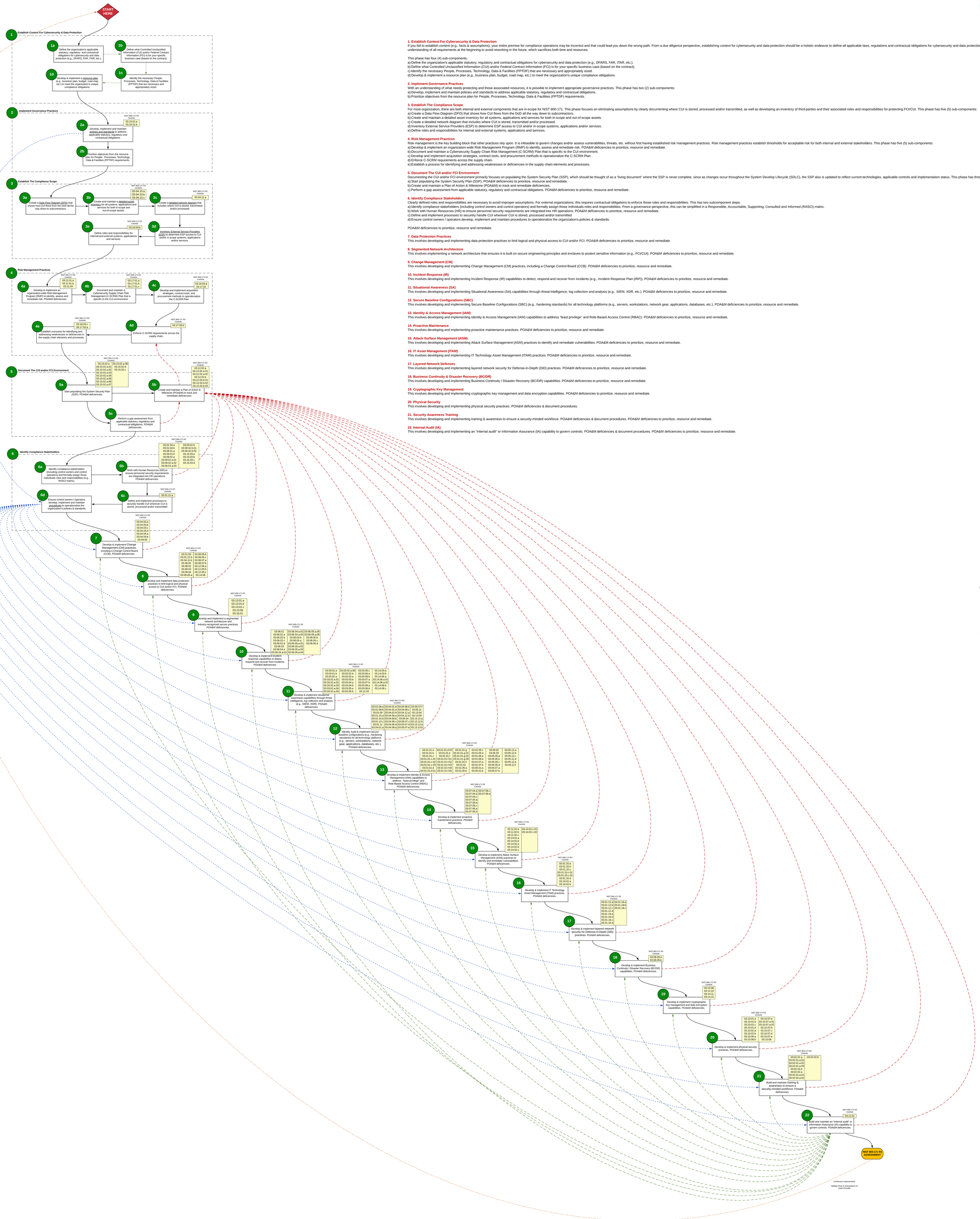
NIST SP 800-171 R3 Kill Chain

version 2024.1

Attribution-NoDerivatives 4.0 International



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 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.

Copyright © 2024 by Compliance Forge, LLC (ComplianceForge). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of ComplianceForge, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of ComplianceForge. Requests may be sent to support@complianceforge.com.