COMPLIANCE FORGE

NIST 800-171 & Cybersecurity Maturity Model Certification (CMMC) Scoping Guide for Controlled Unclassified Information (CUI) & Federal Contract Information (FCI)

CUI Scoping Guide

A Zone-Based Model For A Data-Centric Security Approach To Defining NIST 800-171 & CMMC Scoping

Version 2020.5

Table of Contents

EXECUTIVE SUMMARY

This document is intended to help Organizations Seeking Certifications (OSC) comply with NIST 800-171 and prepare for a Cybersecurity Maturity Model Certification (CMMC) assessment by understanding the scope of its regulated data across its network(s) and service providers. Part of the process of becoming compliant with this regulation is understanding the scope of the **Controlled Unclassified Information (CUI)** and **Federal Contract Information (FCI)** environment.

Given that there are similarities between scoping for NIST 800-171 and the Payment Card Industry Data Security Standard (PCI DSS), we leveraged the outstanding concepts that the **PCI Resources** published in **their PCI DSS Scoping Model and Approach**[1] by applying the scoping methodology to NIST 800-171.

When you look at NIST 800-171 compliance scoping, it has some similarities to PCI DSS:

- PCI DSS is focused on protecting the Cardholder Data Environment (CDE), which is where payment card data is stored, processed and transmitted.
- NIST 800-171 is focused on protecting the CUI/FCI environment, which is where sensitive data (in regard to US national security) is stored, processed or transmitted.
- Both cardholder data and CUI/FCI are considered "infectious" from the perspective of scoping. Without proper segmentation and clear business processes, CUI/FCI "infects" the entire network and greatly expands the scope of compliance and audits.

From the perspective of PCI DSS, if scoping is done poorly, a company's entire network may be in-scope as the CUI, which means PCI DSS requirements would apply uniformly throughout the entire company. In these scenarios, PCI DSS compliance can be prohibitively expensive or even technically impossible. However, when the network is intelligently designed with security in mind, the CDE can be a small fraction of the company's network, which makes compliance much more achievable and affordable. We feel that NIST 800-171 should be viewed in the very same manner.

This guide is not endorsed by the National Institute of Science and Technology (NIST) or any other organization. This is merely an unofficial guide that ComplianceForge compiled to help companies comply with NIST 800-171.

If you are unsure what CUI/FCI is, we highly recommend that you visit the US government's authority on the matter, the **US Archive's CUI Registry** - https://www.archives.gov/cui/registry.

[1] PCI Resources - PCI DSS Scoping Model and Approach https://www.pciresources.com/pci-dss-scoping-model-and-approach/

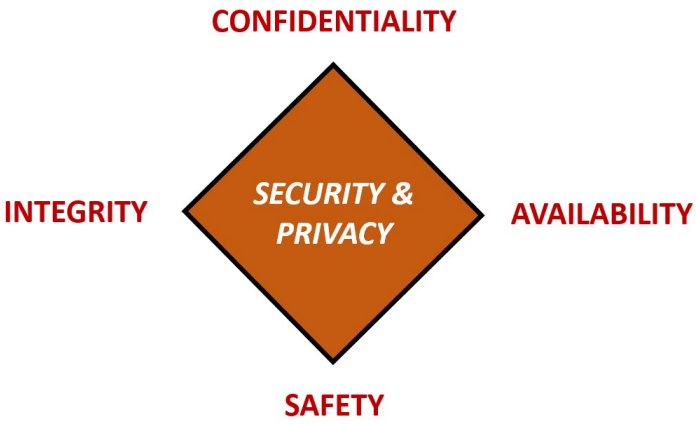
Understanding The Intent of NIST 800-171 & CMMC

If you are new to NIST 800-171, it is intended to help "non-federal entities" (e.g., government contractors) comply with reasonably-expected security requirements by using the systems and practices that government contractors already have in place, rather than trying to use government-specific approaches. CMMC is an independent third-party assessment to help enforce NIST 800-171 compliance.

NIST 800-171 also provides a standardized and uniform set of requirements for all **Controlled Unclassified Information (CUI)** security needs, tailored to non-federal systems, allowing government contractors to comply and consistently implement safeguards for the protection of CUI. When it comes down to it, NIST 800-171 is designed to address common deficiencies in managing and protecting unclassified information.

Addressing Confidentiality, Integrity, Availability & Safety (CIAS)

Protecting the systems that process, store and transmit CUI/FCI is of critical importance. Therefore, safeguards must exist to offset possible threats to the confidentiality, integrity and availability of CUI/FCI and the systems that enable access to it. This used to be considered the "CIA Triad," but now it also has a safety component. This concept forms the foundation of what cybersecurity measures are implemented to protect:



- **Confidentiality** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **Integrity** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **Availability** – Availability addresses ensuring timely and reliable access to and use of information.
- **Safety** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012

DFARS 252.204-7012 establishes the need to protect CUI by providing "adequate" protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. This DFARS clause requires compliance with NIST 800-171 on all "Covered Contractor Information Systems."

- **Covered Contractor Information System (CCIS)** means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits "Covered Defense Information."
- **Covered Defense Information (CDI)** means unclassified "Controlled Technical Information" or other information, as described in the CUI Registry.
- **Controlled Technical Information (CTI)** means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Examples of technical information include, but are not limited to:

- Research and engineering data
- Engineering drawings
- Associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and
- Computer software executable code and source code.

Controlled Unclassified Information (CUI)

NIST 800-171 requires private companies to protect the confidentiality of CUI where it is stored, transmitted and/or processed.

The CUI requirements within NIST 800-171 are directly linked to **NIST 800-53 MODERATE baseline controls** and are intended for use by federal agencies in contracts or other agreements established between those agencies and government/DoD contractors, as it applies to:

- When CUI is resident in non-federal information systems and organizations;
- When information systems where CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and
- Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI category or subcategory listed in the CUI Registry.

Federal Contract Information (FCI)

Federal Acquisition Regulation (FAR) 52.204-31, Basic Safeguarding of Covered Contractor Information Systems, lists fifteen (15) cybersecurity requirements.[2] These requirements form the basis of Cybersecurity Maturity Model Certification (CMMC) Level 1 practices.

Since CMMC addresses both CUI and FCI requirements, both must be adequately scoped, so this guide addresses both CUI and FCI.

Cybersecurity Maturity Model Certification (CMMC)

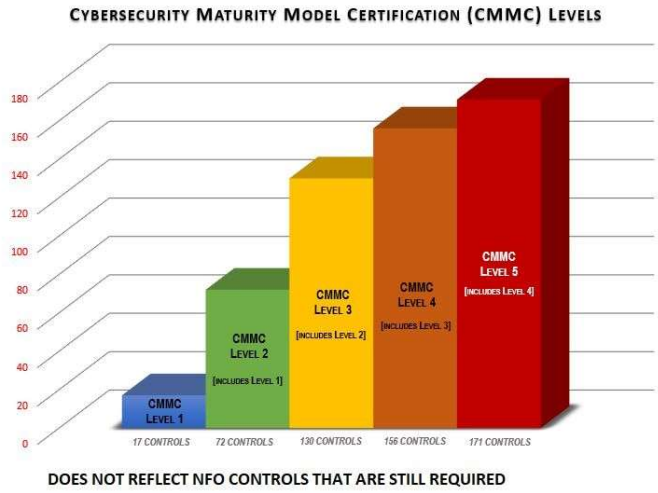
For a more detailed explanation of CMMC, please visit: https://www.complianceforge.com/cybersecurity-maturity-model-certification-cmmc/

CMMC is a vehicle the US Government is using to implement a tiered approach to audit contractor compliance with NIST SP 800-171, based on five different levels of maturity expectations. DoD contractors have been required to comply with NIST 800-171 since January 1, 2018. In the past two years, the DoD grappled with the low rate of NIST 800-171 compliance across the Defense Industrial Base (DIB) and CMMC was created to remedy that systemic issue of non-compliance by both primes and their subs. Interestingly, when NIST 800-171 was initially launched, the DoD would not accept any form of 3rd-party audit for evidence of NIST 800-171 compliance, but that is exactly what CMMC does, so a lot has changed in the past two years from how NIST 800-171 adoption was initially envisioned.

Think of CMMC as a procurement gate that a contractor must pass to even be eligible to bid on, win or participate on a contract - without a valid CMMC certification (Level 1 through 5), the prime and/or sub will be barred from the contract. It is conservatively-estimated that between 200,000-300,000 organizations will be in scope for CMMC, with many of those not being considered traditional defense contractors. The reason for that is the trickle-down effect of third-parties that have the ability to impact the confidentiality and/or integrity of Controlled Unclassified Information (CUI) where it is stored, transmitted and/or processed. This trickle-down will impact small organizations from IT support to bookkeepers and even janitorial support services, in addition to component manufacturers that fall in the supply chain.

Based on version 1.02 of the CMMC, there are 5 levels and each has its own specific set of controls that will be in scope for a CMMC assessment. Each level of CMMC maturity has increasing expectations:

- CMMC Level 1: 17 Controls
- CMMC Level 2: 72 Controls (includes Level 1 controls)
- CMMC Level 3: 130 Controls (includes Level 2 controls)
- CMMC Level 4: 156 Controls (includes Level 3 controls)
- CMMC Level 5: 171 Controls (includes Level 4 controls)



[2] FAR 52.204-21 - https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems

SCOPING NIST 800-171 COMPLIANCE & CMMC ASSESSMENTS

This guide provides a structured methodology for determining which systems, applications and services in a company's IT infrastructure are within scope for NIST 800-171 compliance and CMMC assessments. This guide categorizes system components according to several factors:

- Whether CUI/FCI is being stored, processed or transmitted;
- The functionality that the system component provides (e.g. access control, logging, antimalware, etc.); and
- The connectivity between the system and the CUI/FCI environment.

This NIST 800-171 & CMMC scoping guide can be used by both large and small companies to help critically evaluate the system components that comprise the scope of assessment. The primary difference between large and small companies will be the number of system components that are evaluated.

WHAT THIS GUIDE DOES ADDRESS

Addressing the people, processes and technologies around CUI/FCI is a necessary part of any NIST 800-171 / CMMC compliance program. This guide focuses on categorizing the system components that comprise a company's computing environment and helps with the following:

- Assists in determining which system components fall in and out of scope.
- Facilitates constructive communication between your company and a CMMC assessor by providing a reasonable methodology to describe your technology infrastructure and CUI/FCI environment.
- Provides a means to categorize the various different types of assets, each with a different risk profile associated with it.
- Provides a starting point to potentially reduce the scope of NIST 800-171 and CMMC by re-architecting technologies to isolate and control access to the CUI/FCI environment.
- **Non-Federal Organization (NFO)** controls, found in Appendix E of NIST 800-171, are also included in scoping considerations to identify underlying security practices that are expected to exist. These secure practices support CUI/FCI security activities.[3]

WHAT THIS GUIDE DOES NOT ADDRESS

This guide does not define which NIST 800-171 controls or CMMC practices/processes are required for each category. Since every company is different, it is up to each company and its assessor to determine the nature, extent and effectiveness of each control to adequately mitigate the risks to CUI/FCI.

SEGMENTATION CONSIDERATIONS

It is important to understand that without adequate network segmentation (e.g., a flat network) the entire network is in scope for NIST SP 800-171 and a CMMC assessment. Network segmentation should be viewed as a very beneficial process to isolate system components that store, process or transmit FCI/CUI from systems that do not. Adequate network segmentation may reduce the scope of the FCI/CUI environment and overall reduce the scope of a CMMC assessment.

To eliminate ambiguity surrounding the term "segmentation" in terms of CMMC assessment scoping, this guide uses one of the two following terms:

- **Isolation** – No logical access. This is achieved when network traffic between two assets is not permitted.
- **Controlled Access** – Logical access is permitted. This is achieved when access between assets is restricted to defined parameters.
    - Controlled access is more common than isolation.
    - Restrictions may include logical access control, traffic type (e.g., port, protocol or service), the direction from which the connection is initiated (e.g., inbound, outbound), etc.

Examples of mechanisms that provide controlled access include firewalls, routers, hypervisors, etc.

[3] For more information on NFO controls - https://www.nfo-controls.com/

NIST 800-171 / CMMC Due Diligence & Due Care Steps

Before an OSC uses this guide, it needs to perform the following steps:

1. Document the **System Security Plan (SSP)** to clearly identify what makes up the FCI/CUI environment. This includes dataflows and all instances where CUI is stored, transmitted and processed.
2. Create a **logical network diagram** of your network(s), including any third-party services, cloud instances and remote access methods. Both a high-level and low-level diagram is expected:
    - A high-level diagram can be "cartoonish" to depict broad concepts.
    - A low-level diagram needs to be detailed and identify the ports, protocols and services that are used across the FCI/CUI environment. This information should match what exists in applicable Access Control Lists (ACLs).
3. Document an **inventory of all systems, applications and services** that includes, but is not limited to:
    - Servers
    - Workstations
    - Network devices
    - Mobile devices
    - Databases
    - Third-party service providers
    - Cloud instances
    - Major applications (including what servers and databases they depend on)

***Note**: Failure to adequately perform the three steps listed above should indicate that every system, application and service in the OSC will be considered in scope for NIST SP 800-171 and a CMMC assessment. The old adage of "if you fail to plan, you plan to fail" is very applicable in this scenario.*

Scoping Categories

There is no official guidance or methodology from NIST or the DoD on categorizing assets as being either in or out of the scope for NIST 800-171 / CMMC. Given that lack of guidance and a need for businesses to demonstrate both due care and due diligence with their NIST 800-171 / CMMC compliance operations, ComplianceForge developed this guide that includes eight (8) categories of system components and highlights the different types of risks associated with each category. This approach makes it evident which systems, applications and services must be protected risk posed to CUI.

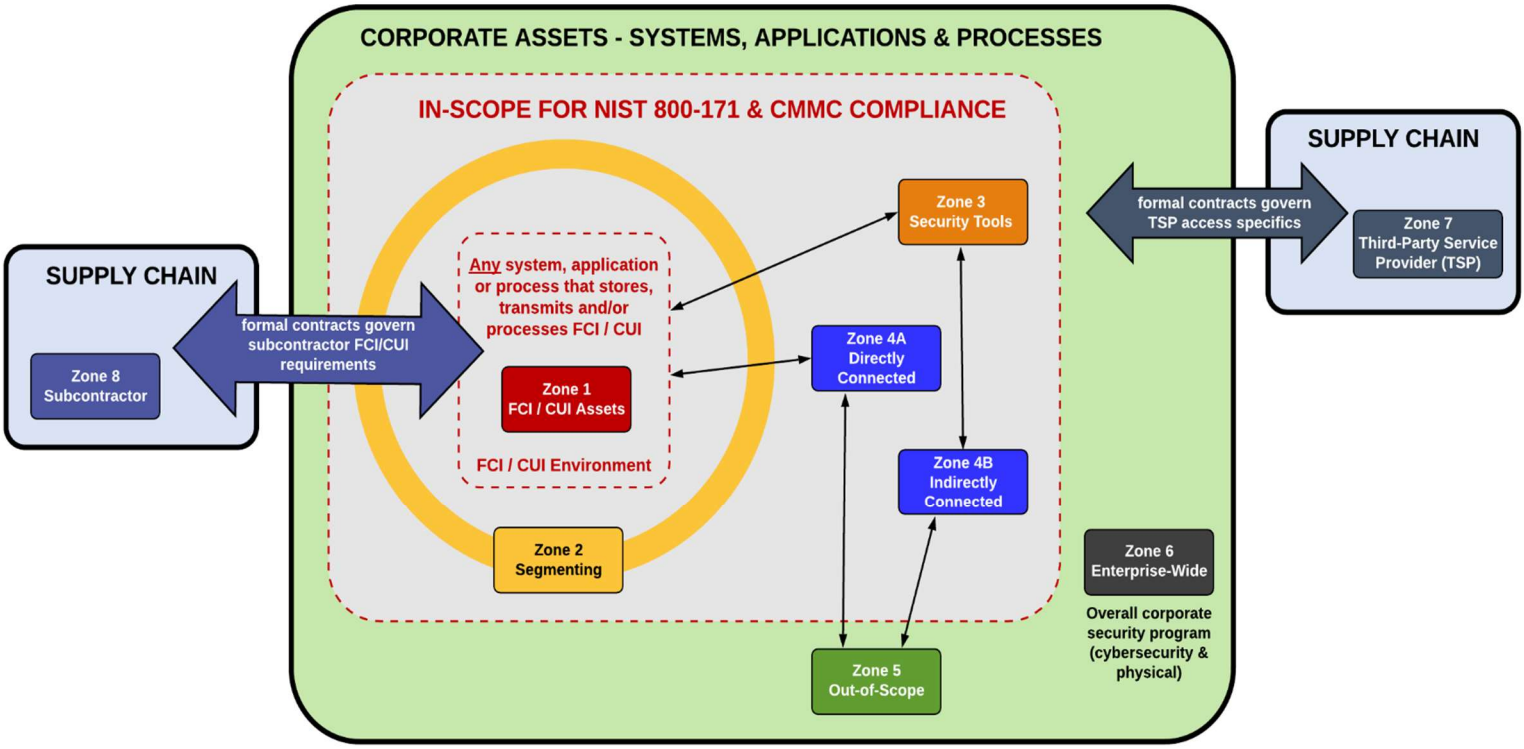
The CUI/FCI environment encompasses the systems, applications and services that store, process and transmit CUI.

- Store – When CUI/FCI is inactive or at rest (e.g., located on electronic media, system component memory, paper)
- Process – When CUI/FCI is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed)
- Transmit – When CUI/FCI is being transferred from one location to another (e.g., data in motion).

Zone-Based Approach To Implementing Data-Centric Security Towards CUI/FCI Assets

When viewing scoping, there are eight (8) zones for NIST 800-171 and CMMC compliance purposes.

1. **CUI/FCI Assets**: The first zone contains systems, services and applications that clearly store, transmit and/or process CUI, CTI or CDI.
2. **Segmenting**: The second zone contains "segmenting systems" that provide access (e.g., firewall, hypervisors, etc.)
3. **Security Tools**: The third zone contains "security tools" that directly impact the integrity of category 1 and 2 assets (e.g., Active Directory, centralized antimalware, vulnerability scanners, IPS/IDS, etc.).
4. **Connected**. The fourth zone contains connected systems. These are systems, applications or services that have some direct or indirect connection into the CUI/FCI environment. Systems, applications and services that may impact the security of (for example, name resolution or web redirection servers) the CUI/FCI environment are always in scope. Essentially, it something can impact the security of the CUI, it is in scope.
5. **Out-of-Scope**. The fifth zone contains out-of-scope systems that are completely isolated from the CUI/FCI systems. For these, always remember that.
6. **Enterprise-Wide**. The sixth zone addresses the organization's overall corporate security program (cyber and physical). This is where the NFO controls are applicable to NIST 800-171 and CMMC compliance.
7. **Third-Party Service Provider**. The seventh zone addresses supply-chain security with the "flow down" of contractual requirements to Third-Party Service Providers (TSPs) that can directly or indirectly influence the CUI/FCI environment. TSPs are third-party organizations that provide services to the OSC.
8. **Subcontractors.** The eighth zone addresses subcontractors, which are third-party organizations that are party to the actual execution of the contract where the subcontractor may create, access, receive, store and/or transmit regulated data (FCI/CUI).



ZONE 1: CUI/FCI ENVIRONMENT

All systems, applications and services that store, transmit and/or process CUI/FCI are Category 1 devices. These systems that interact with CUI/FCI are the main assets that NIST 800-171 and CMMC are trying to protect.

ZONE 2: SEGMENTING

All network devices or hypervisors that provide segmentation functions are Category 2 devices. This category involves systems that provide segmentation and prevent "CUI/FCI contamination" from the CUI/FCI environment to uncontrolled environments. Typically, these are network firewalls that implement some form of Access Control List (ACL) to restrict logical access into and out of the CUI/FCI environment.

Note: If network segmentation is in place and is being used to reduce the scope of NIST 800-171 and a CMMC assessment, expect the assessor to verify that the segmentation is adequate to reduce the scope of the assessment. the more detailed the documentation your assessor will require to adequately review the implemented segmenting solution.

These two NIST 800-171 controls address the concept of segmenting:

- **3.1.3** Control the flow of CUI/FCI in accordance with approved authorizations.
- **3.13.1** Monitor, control, and protect communications (e.g., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

ZONE 3: SECURITY TOOLS

All systems that provide security-related services or IT-enabling services that may affect the security of the CUI/FCI environment are Category 3 devices. There are systems that can impact configurations, security services, logging, etc. that can be in a dedicated security subnet or on the corporate LAN.

These include, but are not limited to:

- Identity and Directory Services (**Active Directory**, **LDAP**)
- Domain Name Systems (**DNS**)
- Network Time Systems (**NTP**)
- Patch management systems
- Vulnerability & patch management systems
- Anti-malware management systems
- File Integrity Management (**FIM**) systems
- Data Loss Prevention (**DLP**) systems
- Performance monitoring systems
- Cryptographic key management systems
- Remote-access or Virtual Private Network (**VPN**) systems
- Multi-factor Authentication (**MFA**) systems
- Mobile Device Management (**MDM**) systems
- Log management and Security Incident Event Management (**SIEM**) systems
- Intrusion Detection Systems/ Intrusion Prevention Systems (**IDS/IPS**)

ZONE 4: CONNECTED

Any system that has some capability to communicate with systems, applications or services within the CUI/FCI environment is a Category 4 device. A “connected” system, application or service should be considered in scope for NIST 800-171 since it is not completely isolated. If it can potentially impact the security of the CUI, it is in scope for NIST 800-171.

There are two sub-categories of connected devices:

- Directly Connected
- Indirectly Connected

ZONE 4-A: DIRECTLY CONNECTED

This sub-category addresses any system that is "connected to" the CUI/FCI environment is considered a directly-connected system. Any system outside of the CUI/FCI environment that is capable of communicating with a system that stores, transmits or processes CUI/FCI (e.g., asset within the CUI/FCI environment) is a Category 4-A device.

Note – For systems outside of the CUI/FCI environment that have periodic outbound connections from the CUI/FCI environment that do not involve the transfer of regulated data (FCI/CUI), there is a case to argue that the system could be ruled out-of-scope since it cannot have an impact on the security of the CUI. In cases like this, some form of Data Loss Prevention (DLP) tool may be warranted to act as a compensating control to further demonstrate how the asset would be out-of-scope.

ZONE 4-B: INDIRECTLY CONNECTED

This sub-category addresses any system that does not have any direct access to CUI/FCI systems (e.g., not interacting with the CUI/FCI environment). Any system that has access to Connected or Segmenting systems and that could affect the security of the CUI/FCI environment is a Category 4-B device.

An example of an indirectly connected system would be that of an administrator's workstation that can administer a security device (Active Directory, firewall, etc.) or upstream system that feeds information to connected systems (e.g. patching system, DNS, etc.). In the case of a user directory, an administrator could potentially grant himself/herself (or others) rights to systems in the CUI/FCI environment, therefore breaching the security controls applicable to the CUI/FCI environment.

ZONE 5: OUT-OF-SCOPE

Any system, application or service that is not a CUI-contaminated, segmenting or connected system is a Category 5 asset. These assets are considered out-of-scope for NIST 800-171 compliance. These out-of-scope assets must be completely isolated (no connections whatsoever) from CUI/FCI systems, though they may interact with connected systems (and can even reside in the same network zone with connected systems).

Four (4) tests must be considered to confirm that a system is out-of-scope and considered a Category 5 asset. This amounts to ensuring that the asset does not fall under the previously defined categories:

1. System components do NOT store, process, or transmit CUI/CTI/CDI.
2. System components are NOT on the same network segment or in the same subnet or VLAN as systems, applications or processes that store, process, or transmit CUI
3. System component cannot connect to or access any system in the CUI/FCI environment.
4. System component cannot gain access to the CUI/FCI environment, nor impact a security control for a system, application or service in the CUI/FCI environment via an in-scope system.

ZONE 6: ENTERPRISE WIDE

This category addresses enterprise-wide security controls that exist outside of just the CUI/FCI environment and specifically addresses Non-Federal Organization (NFO) controls. Within this category are the corporate-wide security practices that affect both cyber and physical security, including security-related policies, standards and procedures that affect the entire organization.

ZONE 7: THIRD-PARTY SERVICE PROVIDER (TSP)

NIST 800-171 and CMMC take supply chain security seriously and this category addresses Third-Party Service Providers (TSPs). The formal contracts between your organization its TSPs dictate the logical and physical access those TSP have to the organization's facilities, systems and data. The "flow down" considerations of NIST 800-171 and CMMC must be addressed with each TSP to clearly identify the TSPs' ability to directly or indirectly influence the CUI/FCI environment.

Examples of TSPs that must comply with CMMC practices:

- Landscapers
- Bookkeepers
- Human Resource (HR) recruiters
- Payroll providers
- Educational training providers
- IT service providers

- Security consultants
- Business process consultants
- Project Managers (PMs)
- Document destruction providers
- Janitorial services
- Any organization that provides administration of or monitors assets within an organization's CUI/FCI Environment

Zone 8: Subcontractor

ZONE 8
SUBCONTRACTOR

This category addresses subcontractors necessary to perform the in-scope contract. While a subcontractor is a third-party, a subcontractor is party to the actual execution of the contract where the subcontractor may create, access, receive, store and/or transmit regulated data (FCI/CUI).

In-Scope Matrix

The following chart summarizes the concept of what is and is not in scope:

Type	Segmentation Method	CUI / FCI Data?	In Scope?
Zone 1 CUI Assets	None	YES	YES
Zone 2 Segmenting	Provides Segmentation	NO	YES
Zone 3 Security Tools	Controlled Access	NO	YES
Zone 4 Connected	Controlled Access	NO	YES
Zone 4-A Directly Connected	Controlled Access	NO	YES
Zone 4-B Indirectly Connected	Indirect Access	NO	YES
Zone 5 Out-of-Scope	Isolated	NO	NO
Zone 6 Enterprise Wide	N/A - Applicable To The Entire Organization	NO	NO
Zone 7 TSPs	Must Be Determined	MAYBE	MAYBE
Zone 8 Subcontractors	Must Be Determined	YES	YES

System-to-System Communications

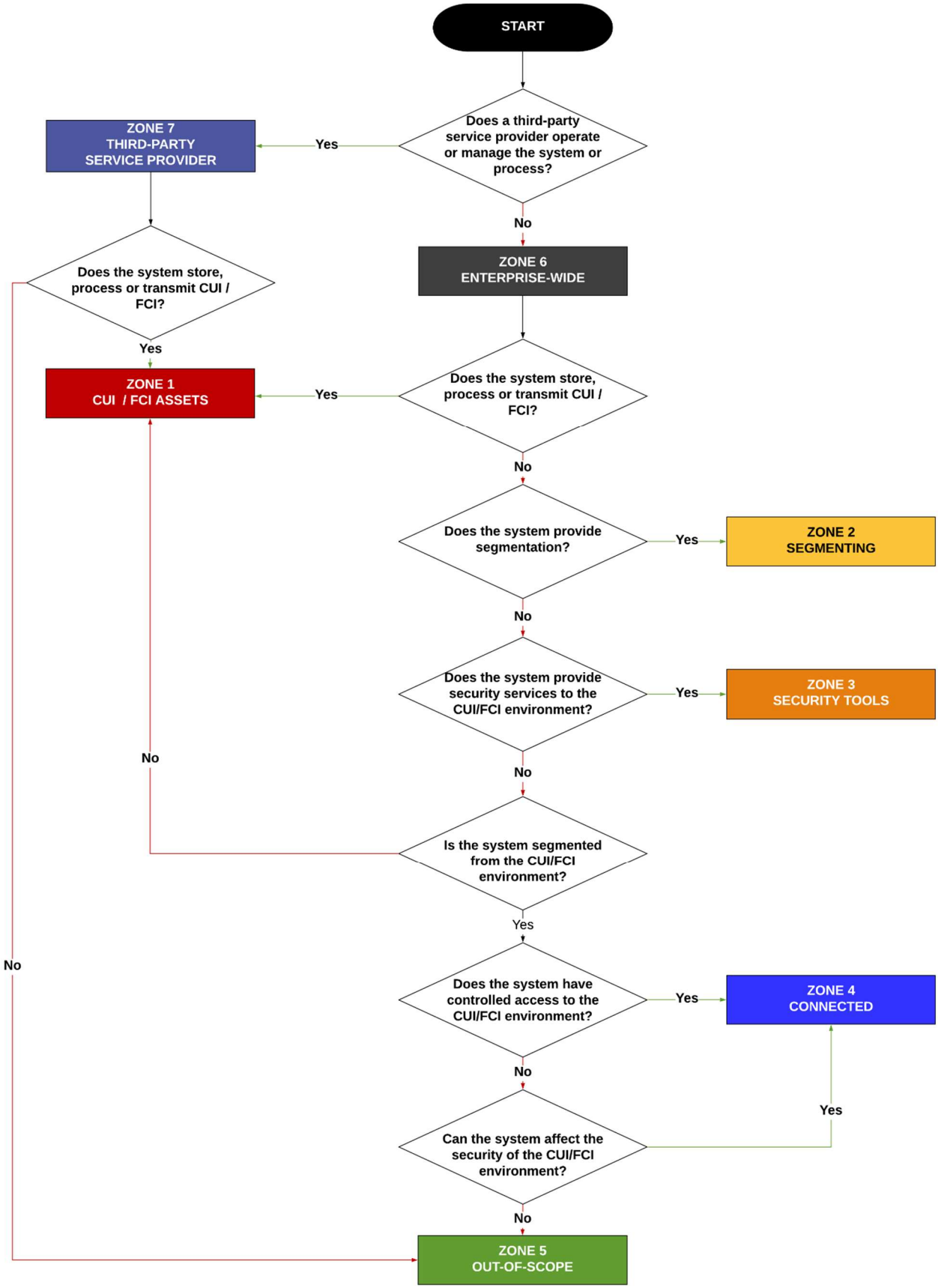
The following chart summarizes the concept of what communications are or are not in-scope for NIST 800-171/CMMC.

Communications In Scope For NIST 800-171 & CMMC?	Zone 1 CUI / FCI Assets	Zone 2 Segmenting	Zone 3 Security Tools	Zone 4 Connected	Zone 5 Out-of-Scope	Zone 6 Enterprise Wide	Zone 7 TSPs	Zone 8 Subcontractors
Zone 1 CUI / FCI Assets	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	NO *Isolated*	NO *Isolated*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*
Zone 2 Segmenting	IN-SCOPE *CUI /FCI Environment*	Possibly *Controlled Access*	Possibly *Controlled Access*	Possibly *Controlled Access*	NO *Isolated*	NO *Isolated*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*
Zone 3 Security Tools	IN-SCOPE *CUI /FCI Environment*	Possibly *Controlled Access*	Possibly *Controlled Access*	Possibly *Controlled Access*	NO *Isolated*	NO *Isolated*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*
Zone 4 Connected	IN-SCOPE *CUI /FCI Environment*	Possibly *Controlled Access*	Possibly *Controlled Access*	Possibly *Controlled Access*	NO *Isolated*	NO *Isolated*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*
Zone 5 Out-of-Scope	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*
Zone 6 Enterprise Wide	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*	NO *Isolated*
Zone 7 TSPs	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	NO *Isolated*	NO *Isolated*	NO *Isolated*	Possibly *Controlled Access*
Zone 8 Subcontractors	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	IN-SCOPE *CUI /FCI Environment*	NO *Isolated*	NO *Isolated*	Possibly *Controlled Access*	IN-SCOPE *CUI /FCI Environment*

Note – For systems outside of the CUI/FCI environment that have periodic outbound connections from the CUI/FCI environment that do not involve the transfer of regulated data (FCI/CUI), there is a case to argue that the system could be ruled out-of-scope since it cannot have an impact on the security of the CUI.

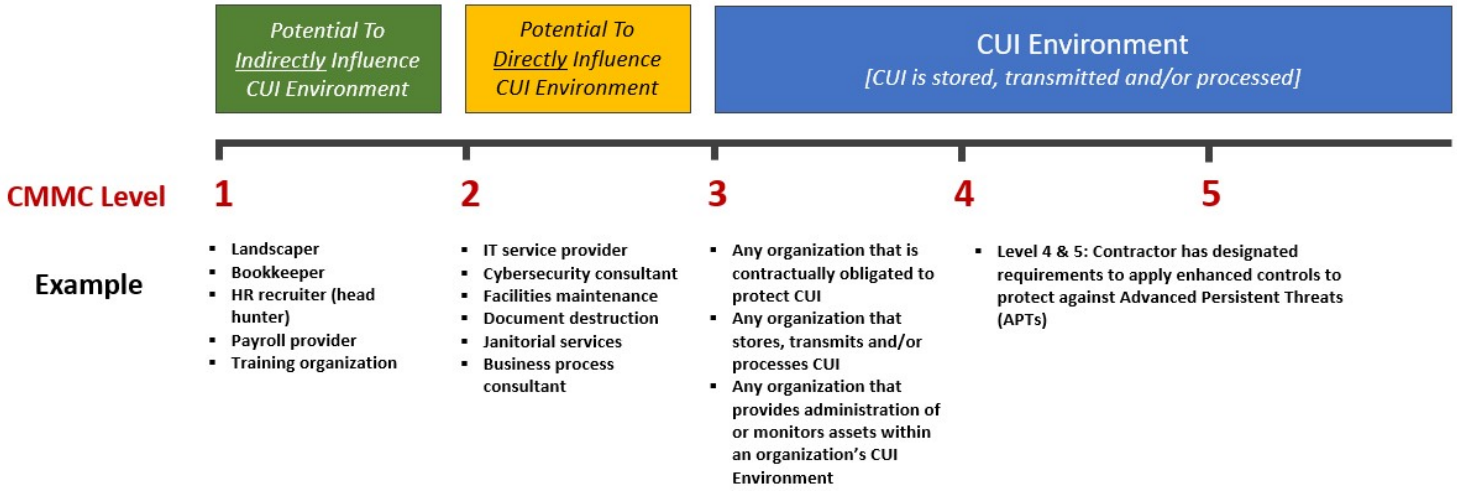
CUI/FCI Scoping Decision Tree

The following decision tree provides a logical walk-through to determine if an asset is in scope or not:

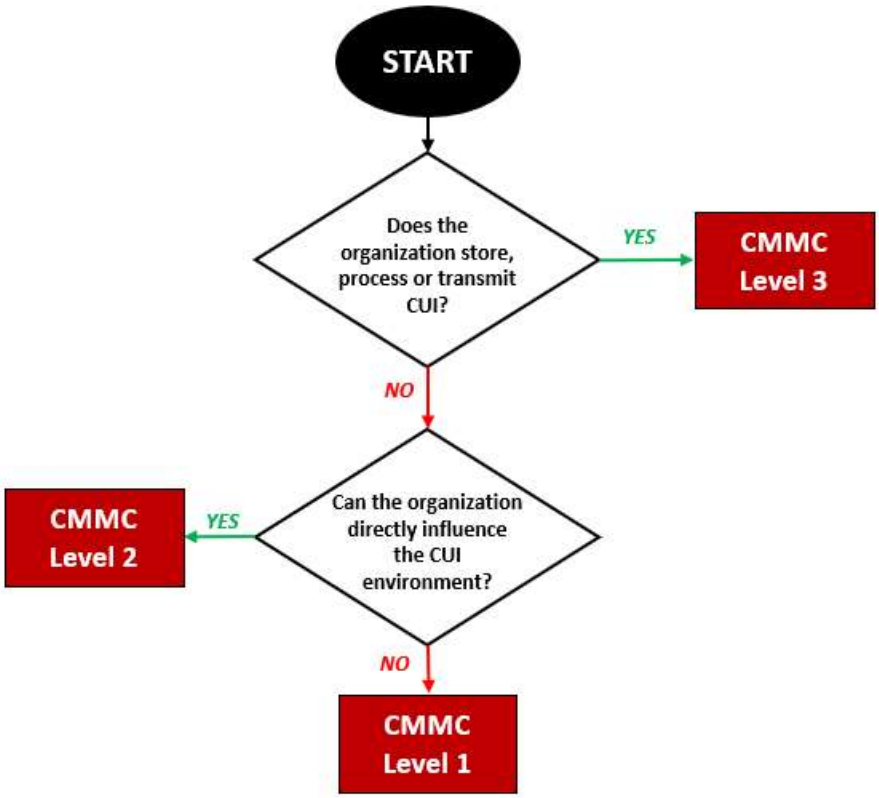


TSP & Subcontractor Scoping Decision Tree – "Flow Down" Considerations

The following criteria is guidance to determine the level of compliance that any TSP / subcontractor must address from a requirements "flow down" perspective. This concept can be applied from a prime to a sub or a sub to TSPs. The concept is based on data-centric security, where the security of the regulated data (FCI/CUI) drives the requirements.



The following decision tree provides a logical walk-through to help determine what CMMC level a TSP /subcontractor needs should comply with:



Example Network Scoping Scenarios

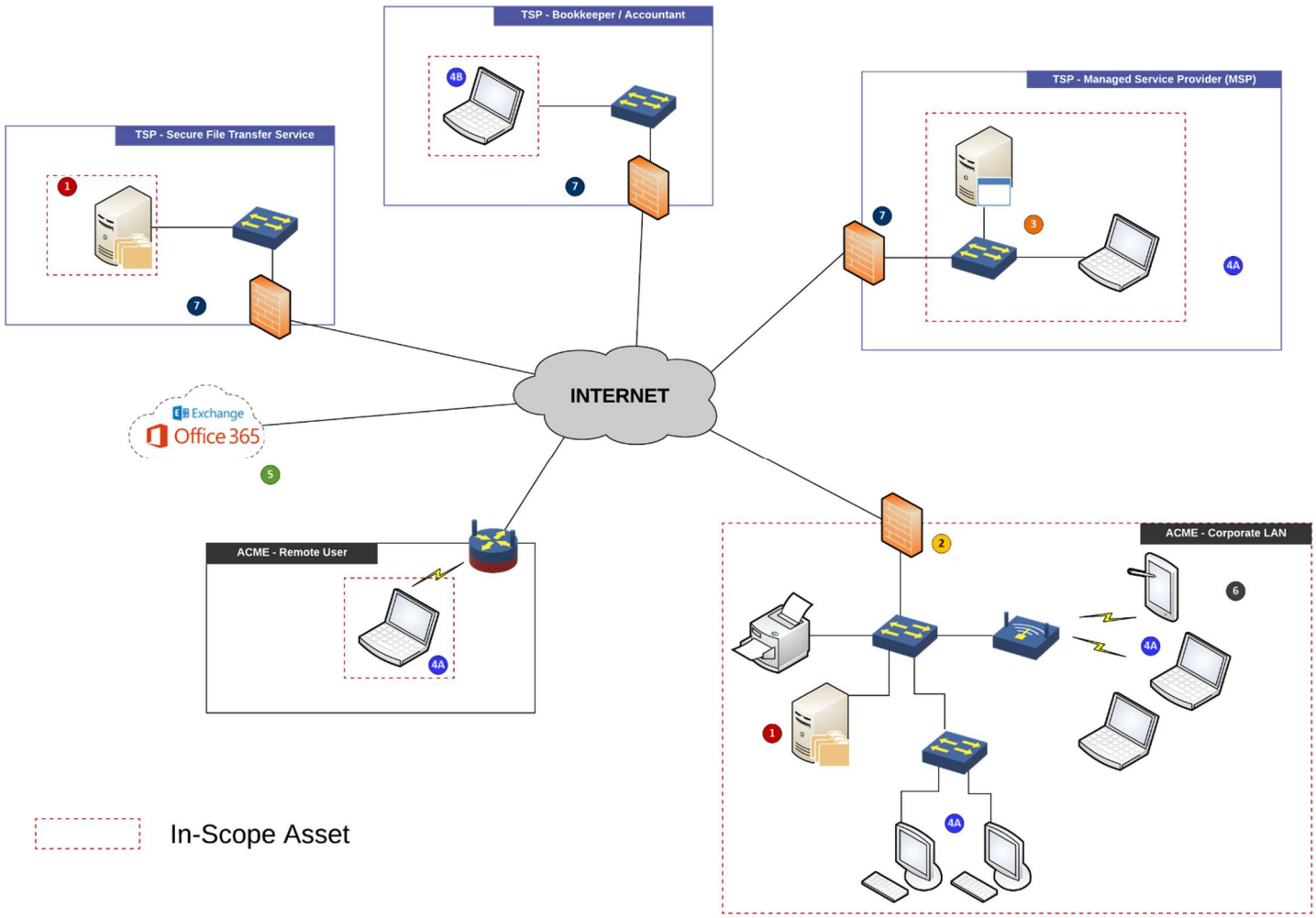
These scenarios are for reference purposes only to help you visualize walking through your data flows and network diagrams to identify what assets are in-scope and what is out-of-scope.

Scenario 1: Flat Network

In this scenario, ACME Consulting (ACME) is the OSC and is a subcontractor on a project to manufacture an antenna for a DoD weapons system. The dimensions of the antenna are categorized as CUI by the DoD and the design specifications for the components "flow down" to ACME as part of the contract clause.

Background Scenario Details:

- ACME is a Level 3 organization, since it stores, transmits and processes CUI.
- While ACME is able to manufacture all aspects of the shipping crate in-house, it does not have a dedicated IT, cybersecurity or administrative staff, so it relies on Third-Party Service Providers (TSP) for bookkeeping and technology support.
- ACME utilizes a "flat" network without dedicated subnets for CUI.
- ACME does have remote users who must connect via VPN to access corporate resources.
- ACME utilizes a secure file transfer service to send/receive CUI.
- ACME uses Office 365 for email (Exchange) but administratively prohibits CUI from being communicated by email.
- ACME's bookkeeper/accountant can remotely connect into ACME's corporate LAN to work on accounting software through a VPN.
- ACME's Managed Service Provider (MSP) performs patch management and monitoring services for ACME's servers and workstations. IT technicians are able to VPN into the corporate LAN to perform maintenance functions.
- No "jump hosts" are used for the bookkeeper/accountant or the MSP. Those organizations use their own devices to establish the VPN and conduct their duties.



Scoping Exercise:

This scoping exercise identifies the various components of ACME that would be in scope for a Level 3 assessment. Due to a lack of segmentation, not only does all of ACME's network fall within scope, but it involves third-party services and providers.

OSC – Corporate LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
- ACME has a single firewall that connects to the Internet Service Provider (ISP) (**zone 2**).
- ACME utilizes a Network Attached Storage (NAS) device to store CUI (**zone 1**).
- Several OSC users have CUI on their workstations (**zone 1**). However, the majority of the OSC's users do not have CUI their workstations, but due to a lack of segmentation, all corporate assets are in-scope (**zone 4a**).
- Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zone 5**).

OSC – Remote User

- Remote users use a secure VPN tunnel to connect to the ACME corporate LAN.
- The remote users are in scope (**zone 4a**), since there is no segmentation on the corporate LAN.

Managed Service Provider (MSP)

- IT technicians from the MSP use a secure VPN tunnel to connect to the ACME corporate LAN.
- Firewall rules allow MSP monitoring and maintenance services to access ACME's corporate LAN.
- ACME has a written contract with the MSP that documents its security-related roles and responsibilities for the MSP (**zone 7**).
- IT technicians directly connect to ACME assets that have access to systems that store, transmit and process CUI (**zone 4a**) and fall within scope for the Level 3 assessment.
- The "security tools" the MSP uses protect ACME's corporate LAN have direct access to devices that store, transmit and process CUI (**zone 3**). This includes but is not limited to:
    - Patch management
    - Antimalware server
    - Log server (e.g., Security Incident Event Manager (SIEM))

Outsourced Bookkeeper / Accountant

- Bookkeeper / accountant uses a secure VPN tunnel to connect to the ACME corporate LAN and a Remote Desktop Connection (RDC) to perform accounting duties.
- ACME has a written contract with the bookkeeper/accountant (**zone 7**).
- Bookkeeper / accountant assets directly connect to ACME assets that have access to systems that store, transmit and process CUI (**zone 4b**) and fall within scope for the Level 3 assessment.

Secure File Transfer Service

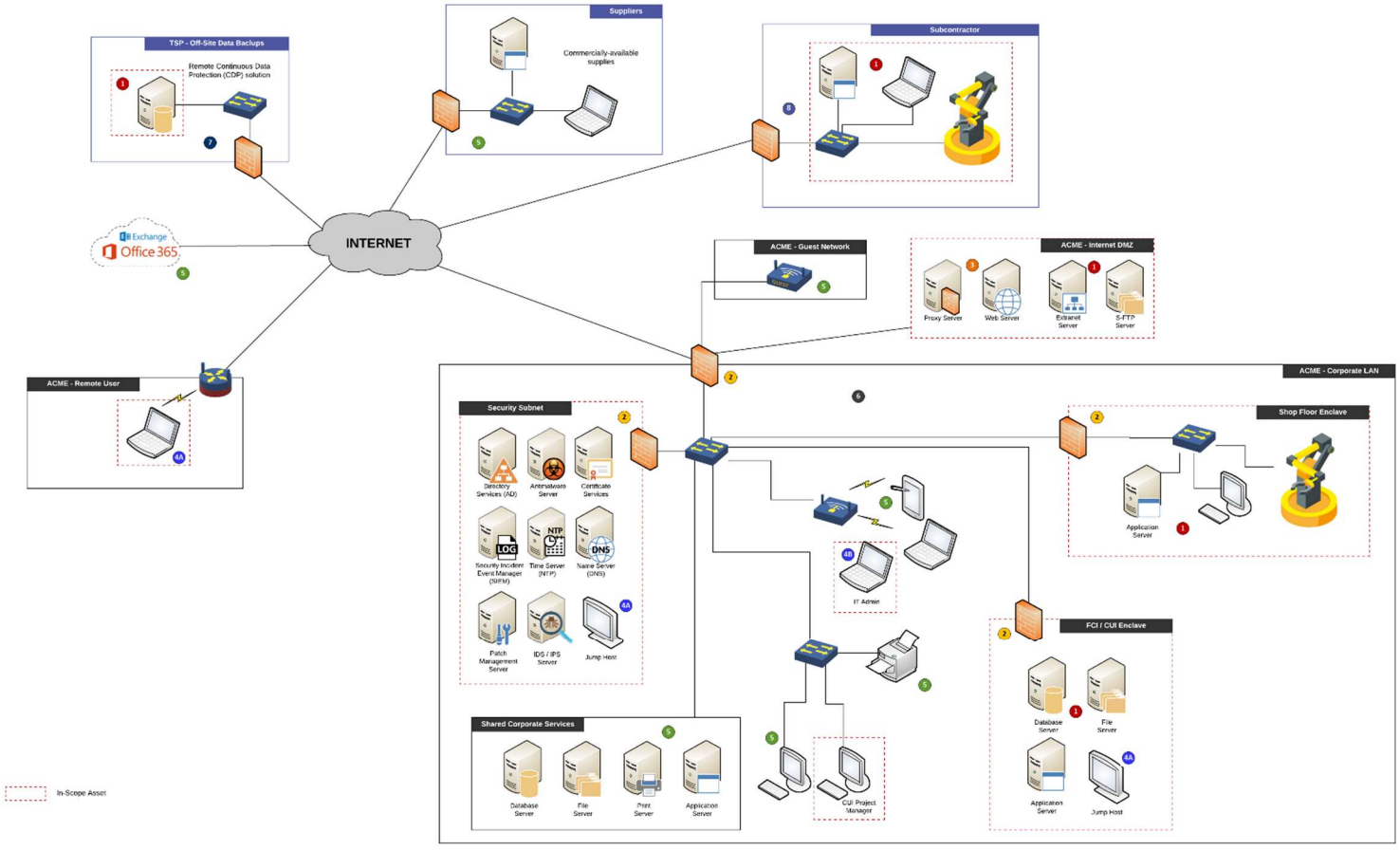
- Due to CUI being temporarily stored and transmitted in the file transfer service's systems, that takes that service within scope (**zone 1**). While the CUI is encrypted in transit, applicable controls need to be reviewed and applied for instances where CUI may be at rest and accessible by MSP personnel.
- ACME has a written contract with the MSP that documents its security requirements (**zone 7**).
- The TSP is excluded from additional controls, since due to the technology it uses, it does not have access to view or modify any data within ACME's service.
- The OSC must secure the secure file transfer service by implementing applicable CMMC controls associated with access control to appropriately protect the data being housed offsite.

Scenario 2: Segmented Network (On-Premise Infrastructure)

In this scenario, ACME Engineering (ACME) is the OSC and is a subcontractor on a project to develop components for a DoD weapons system. The components are categorized as CUI by the DoD and the design specifications for the components "flow down" to ACME as part of the contract clause.

Background Scenario Details:

- ACME is a Level 3 organization, since it stores, transmits and processes CUI.
- ACME relies on subcontractors (sub-subcontractor to the DoD) to manufacture certain subcomponents and the design specifications are shared with the subcontractors.
- ACME uses an extranet (hosted in its DMZ) to securely share design specifications and project updates with the prime and its subcontractors.
- ACME uses Office 365 for email (Exchange) but administratively prohibits CUI from being communicated by email.
- Within ACME's corporate LAN, there are three enclaves:
    1. A "security subnet" where it hosts security-related services for the entire organization;
    2. A specifically designed CUI enclave, where CUI data is hosted to segment it from the rest of the network;
    3. A "shop floor" enclave where manufacturing activities occur, since the CNC machines need the specifications to manufacture the components.
- ACME does have remote users who must connect via VPN to access corporate resources.
- ACME utilizes a remote, Continuous Data Protection (CDP) service to backup its data, which includes CUI.
- ACME uses several suppliers, but it does not share CUI with the suppliers. The items it purchases are all commercially available.



SCOPING EXERCISE:

This scoping exercise identifies the various components of ACME that would be in scope for a Level 3 assessment.

OSC – CORPORATE LAN

- **Corporate LAN**
  - Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
  - The majority of the OSC's corporate LAN (wired & wireless) are out-of-scope (**zone 5**) due to segmentation.
  - Corporate users needing access into a subnet that contains CUI must connect to a "jump host" within that enclave. Those specific assets connecting to the jump box are in-scope (**zone 4b**).
  - Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zone 5**).
- **CUI Enclave**
  - The firewall that provides segmentation services to the CUI enclave is in scope (**zone 2**).
  - The database, file and application server all store, transmit and process CUI (**zone 1**).
  - The jump host directly connects to zone 1 assets, so it is in scope (**zone 4a**).
- **Shop Floor Enclave**
  - The firewall that provides segmentation services to the shop floor enclave is in scope (**zone 2**).
  - The application server stores, transmits and processes CUI (**zone 1**).
  - The manufacturing workstation and CNC machines stores, transmits and processes CUI (**zone 1**).
- **Security Subnet**
  - The firewall that provides segmentation services to the security subnet is in scope (**zone 2**).
  - The jump host directly connects to zone 3 assets, so it is in scope (**zone 4a**).
  - The "security tools" that protect both the corporate LAN and enclave is in scope (**zone 3**). This includes but is not limited to:
    - Directory service (e.g., Active Directory)
    - Patch management
    - Antimalware server
    - Certificate server (e.g., PKI & certificate services)
    - Log server (e.g., Security Incident Event Manager (SIEM))
    - Time server (e.g., Network Time Protocol (NTP))
    - Domain Name Services (DNS)
    - Intrusion Detection / Prevention (IDS/IPS)
- **Shared Services**
  - The "shared services" is an extension of the corporate LAN with non-CUI servers, print servers and application servers that are not in-scope (**zone 5**).

OSC – INTERNET DMZ & GUEST NETWORK

- The Internet DMZ is in scope since it contains an extranet server that is used to store, transmit and process CUI (**zone 1**) and the proxy server is in-scope (**zone 3**) since it provides security services.
- The "guest network" is segmented from the corporate LAN and is out-of-scope (**zone 5**).

OSC – REMOTE USER

- The remote users are not in scope (**zone 5**), since they do not have access to CUI.
- Remote users must use a secure VPN tunnel to connect to the corporate LAN.
- Remote users needing access into a subnet that contains CUI must connect to a "jump host" within that enclave.

THIRD-PARTY SERVICE PROVIDER (TSP) - SECURE FILE TRANSFER SERVICE

- Due to CUI being stored in the off-site backups, that takes that service within scope (**zone 1**).
- TSP has a written contract with ACME that documents its security requirements (**zone 7**).
- The TSP is excluded from additional controls, since it has no access to the private key that encrypts the backed up data.
- The OSC must secure the secure file transfer service by implementing CMMC controls associated with access control and multifactor authentication to appropriately protect the data being housed offsite.

SUBCONTRACTORS

- Since ACME requires specialized subcomponents to be made by subcontractors, it must share CUI with them and that takes the subcontractors within scope (**zone 1**).
- ACME has a written contract with its subcontractors that documents the security requirements to protect CUI (**zone 8**).

SUPPLIERS

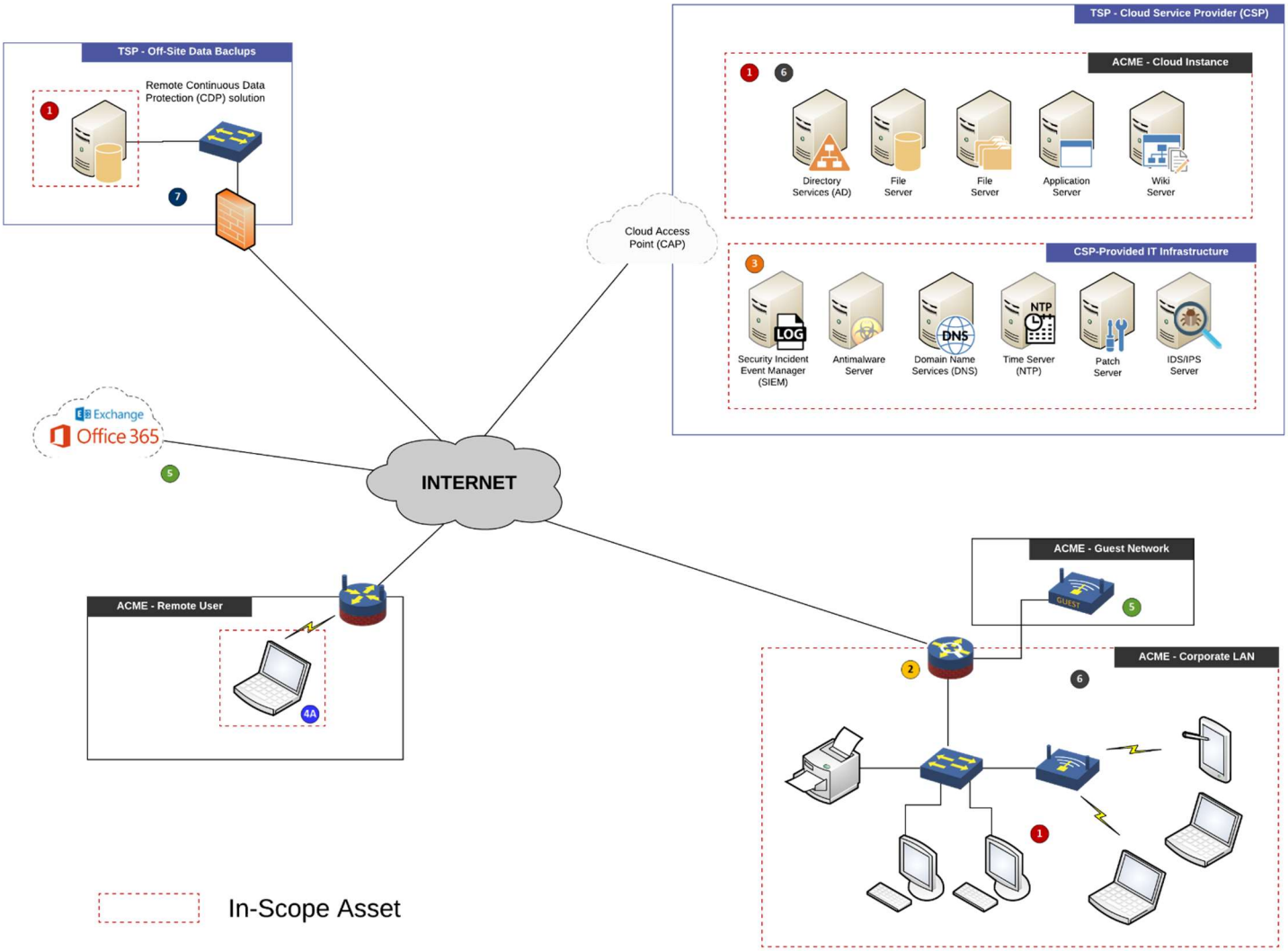
- Since ACME buys commercially available material and does not share CUI with its suppliers, they are out-of-scope (**zone 5**).

Scenario 3: Virtual Network (Cloud Infrastructure)

In this scenario, ACME Staffing (ACME) is the OSC and is a subcontractor on a project to perform project management and consulting for a DoD weapons system. The services ACME provides relies on referencing CUI and the information needed to perform their duties "flow down" to ACME as part of the contract clause.

Background Scenario Details:

- ACME is a Level 3 organization, since it stores, transmits and processes CUI.
- ACME does not have any subcontractors, but it does leverage a "remote workforce" where there is no traditional headquarters building since all the consultants (employees and contractors) work on-site at military installations or at the prime contractor's facilities. The "corporate LAN" is nothing more than a few laptops and a printer in a small office with a basic ISP Internet connection with no guest network or DMZ.
- ACME uses Google for email (G Suite) but administratively prohibits CUI from being communicated by email.
- ACME does have remote users who must connect via VPN to access corporate resources.
- ACME utilizes a remote, Continuous Data Protection (CDP) service to backup its data, which includes CUI.
- ACME utilizes a Cloud Service Provider (CSP) to host its technology infrastructure. It also uses CSP-provided services such as DNS, directory services, NTP, etc. in order to enable the cloud instance to operate.



SCOPING EXERCISE:

This scoping exercise identifies the various components of ACME that would be in scope for a Level 3 assessment.

OSC – CORPORATE LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
- All IT assets on the OSC's corporate LAN (wired & wireless) are in-scope either due to storing, transmitting and/or processing CUI (**zone 1**) or due to a lack of segmentation (**zone 4**).
- ACME has a single firewall that connects to the Internet Service Provider (ISP) (**zone 2**).
- Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zone 5**).

OSC – REMOTE USER

- Remote users use a secure VPN tunnel to connect to the ACME corporate LAN and cloud-based resources.
- The remote users are in scope either due to storing, transmitting and/or processing CUI (**zone 1**) or due to a lack of segmentation (**zone 4**).

THIRD-PARTY SERVICE PROVIDER (TSP) - SECURE FILE TRANSFER SERVICE

- Due to CUI being stored in the off-site backups, that takes that service within scope (**zone 1**).
- TSP has a written contract with ACME that documents its security requirements (**zone 7**).
- The TSP is excluded from additional controls, since it has no access to the private key that encrypts the backed up data.
- The OSC must secure the secure file transfer service by implementing CMMC controls associated with access control and multifactor authentication to appropriately protect the data being housed offsite.

CLOUD SERVICE PROVIDER (CSP)

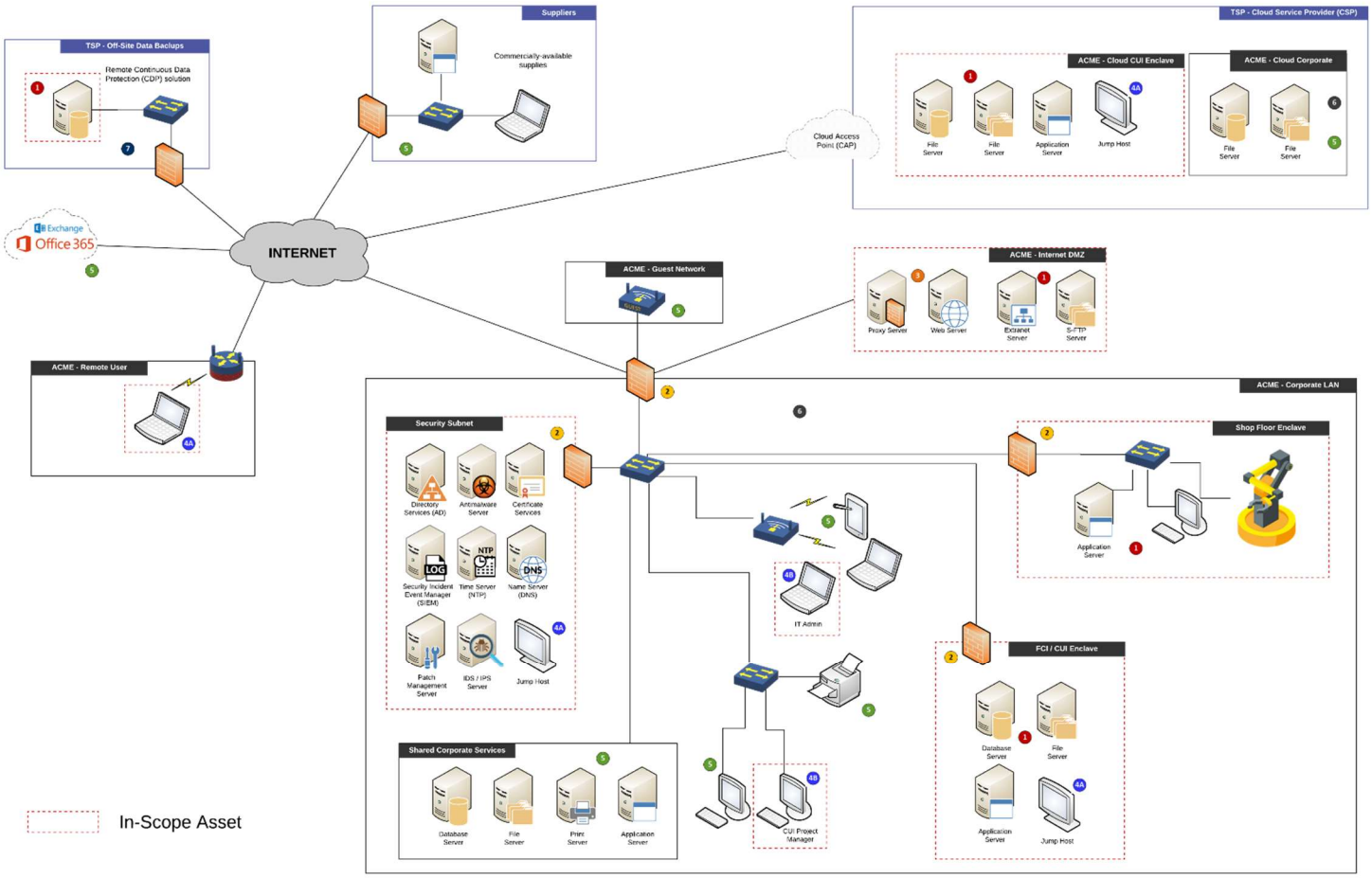
- Firewall rules to the CSP are in-scope (**zone 2**).
- All IT assets on the OSC's cloud instance are in-scope either due to storing, transmitting and/or processing CUI (**zone 1**) or due to a lack of segmentation (**zone 4**).
- CSP has a written contract with ACME that documents its security requirements (**zone 7**). CSP has a clearly-documented demarcation for the specific CMMC/NIST 800-171-related controls that it performs as part of its service offering.
- The "security tools" that protect both the OSC's cloud instance are in-scope (**zone 3**). This includes but is not limited to:
    - Directory service (e.g., Active Directory)
    - Patch management
    - Antimalware server
    - Certificate server (e.g., PKI & certificate services)
    - Log server (e.g., Security Incident Event Manager (SIEM))
    - Time server (e.g., Network Time Protocol (NTP))
    - Domain Name Services (DNS)
    - Intrusion Detection / Prevention (IDS/IPS)

SCENARIO 4: HYBRID NETWORK (ON-PREMISE & CLOUD INFRASTRUCTURE)

In this scenario, ACME Engineering (ACME) is the OSC and is a subcontractor on a project to develop components for a DoD weapons system. The components are categorized as CUI by the DoD and the design specifications for the components "flow down" to ACME as part of the contract clause.

BACKGROUND SCENARIO DETAILS:

- ACME is a Level 3 organization, since it stores, transmits and processes CUI.
- ACME does not rely on any subcontractors and does not share CUI with any organization other than the prime.
- ACME leverages a hybrid IT infrastructure that is split between on-premise and cloud-based assets.
- Within ACME's corporate LAN, there are three enclaves:
    1. A "security subnet" where it hosts security-related services for the entire organization;
    2. A specifically designed CUI enclave, where CUI data is hosted to segment it from the rest of the network;
    3. A "shop floor" enclave where manufacturing activities occur, since the CNC machines need the specifications to manufacture the components.
- Within ACME's cloud instance, there are two enclaves:
    1. A specifically designed CUI enclave, where CUI data is hosted to segment it from the rest of the cloud instance; and
    2. A corporate enclave that contains non-CUI data.
- ACME uses Office 365 for email (Exchange) but administratively prohibits CUI from being communicated by email.
- ACME does have remote users who must connect via VPN to access corporate resources.
- ACME utilizes a remote, Continuous Data Protection (CDP) service to backup its data, which includes CUI.
- ACME uses several suppliers, but it does not share CUI with the suppliers. The items it purchases are all commercially available.



SCOPING EXERCISE:

This scoping exercise identifies the various components of ACME that would be in scope for a Level 3 assessment.

OSC – CORPORATE LAN

- **Corporate LAN**
  - Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
  - The majority of the OSC's corporate LAN are out-of-scope (**zone 5**) due to segmentation.
  - Corporate users needing access into a subnet that contains CUI must connect to a "jump host" within that enclave. Those specific assets connecting to the jump box are in-scope (**zone 4b**).
  - Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zone 5**).
- **CUI Enclave**
  - The firewall that provides segmentation services to the CUI enclave is in scope (**zone 2**).
  - The database, file and application server all store, transmit and process CUI (**zone 1**).
  - The jump host directly connects to zone 1 assets, so it is in scope (**zone 4a**).
- **Shop Floor Enclave**
  - The firewall that provides segmentation services to the shop floor enclave is in scope (**zone 2**).
  - The application server stores, transmits and processes CUI (**zone 1**).
  - The manufacturing workstation and CNC machines stores, transmits and processes CUI (**zone 1**).
- **Security Subnet**
  - The firewall that provides segmentation services to the security subnet is in scope (**zone 2**).
  - The jump host directly connects to zone 3 assets, so it is in scope (**zone 4a**).
  - The "security tools" that protect both the corporate LAN and enclave is in scope (**zone 3**). This includes but is not limited to:
    - Directory service (e.g., Active Directory)
    - Patch management
    - Antimalware server
    - Certificate server (e.g., PKI & certificate services)
    - Log server (e.g., Security Incident Event Manager (SIEM))
    - Time server (e.g., Network Time Protocol (NTP))
    - Domain Name Services (DNS)
    - Intrusion Detection / Prevention (IDS/IPS)
- **Shared Services**
  - The "shared services" is an extension of the corporate LAN with non-CUI servers, print servers and application servers that are not in-scope (**zone 5**).

OSC – INTERNET DMZ & GUEST NETWORK

- The Internet DMZ is in scope since it contains an extranet server that is used to store, transmit and process CUI (**zone 1**) and the proxy server is in-scope (**zone 3**) since it provides security services.
- The "guest network" is segmented from the corporate LAN and is out-of-scope (**zone 5**).

OSC – REMOTE USER

- The remote users are not in scope (**zone 5**), since they do not have access to CUI.
- Remote users must use a secure VPN tunnel to connect to the corporate LAN.
- Remote users needing access into a subnet that contains CUI must connect to a "jump host" within that enclave (**zone 4a**).

OSC – CORPORATE LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
- All IT assets on the OSC's corporate LAN (wired & wireless) are in-scope either due to storing, transmitting and/or processing CUI (**zone 1**) or due to a lack of segmentation (**zone 4**).
- ACME has a single firewall that connects to the Internet Service Provider (ISP) (**zone 2**).

THIRD-PARTY SERVICE PROVIDER (TSP) - SECURE FILE TRANSFER SERVICE

- Due to CUI being stored in the off-site backups, that takes that service within scope (**zone 1**).
- TSP has a written contract with ACME that documents its security requirements (**zone 7**).
- The TSP is excluded from additional controls, since it has no access to the private key that encrypts the backed up data.
- The OSC must secure the secure file transfer service by implementing CMMC controls associated with access control and multifactor authentication to appropriately protect the data being housed offsite.

CLOUD SERVICE PROVIDER (CSP)

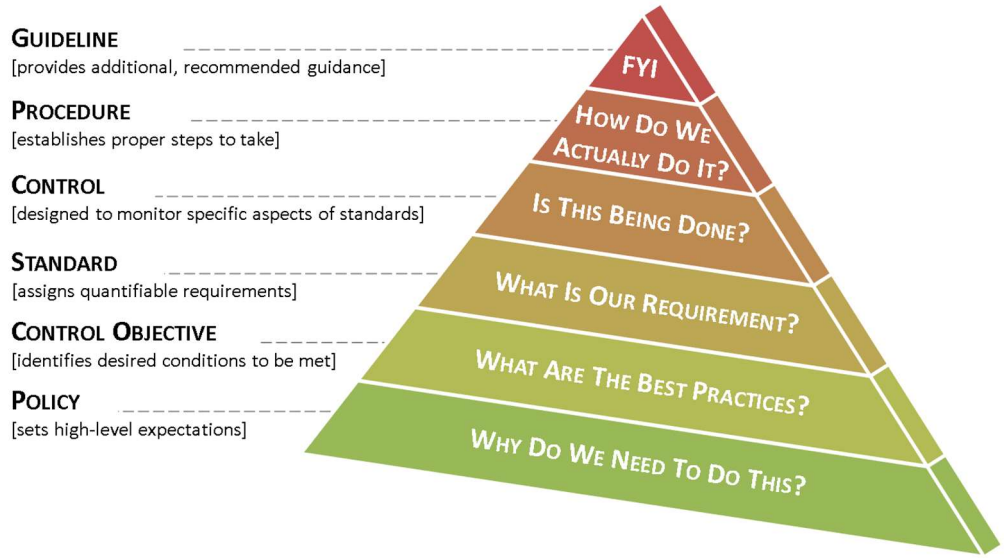
- Firewall rules to the CSP are in-scope (**zone 2**).
- The CUI enclave in the cloud instance is in-scope due to storing, transmitting and/or processing CUI (**zone 1**) and remote users needing access must connect to a "jump host" within that enclave (**zone 4a**).
- The CUI enclave for corporate IT assets that do not contain CUI in the cloud instance is out-of-scope (**zone 5**)
- CSP has a written contract with ACME that documents its security requirements (**zone 7**). CSP has a clearly-documented demarcation for the specific CMMC/NIST 800-171-related controls that it performs as part of its service offering.

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

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

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

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



CYBERSECURITY DOCUMENTATION COMPONENTS

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

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

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

NIST 800-171 In a Nutshell

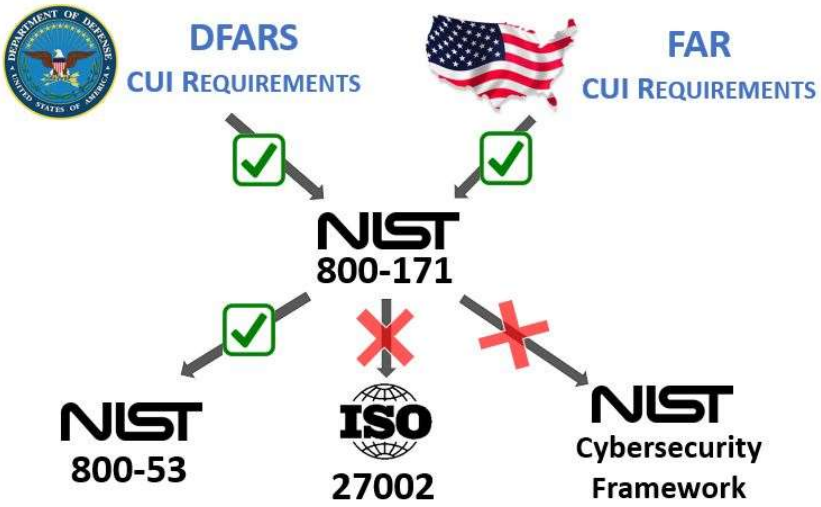
When you break down NIST 800-171 CUI/FCI requirements into how they are operationalized by people, processes or technology, you see that there are a lot of controls that are either administrative or related to technical configurations. Very few realistically require the purchase of new hardware or software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

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

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

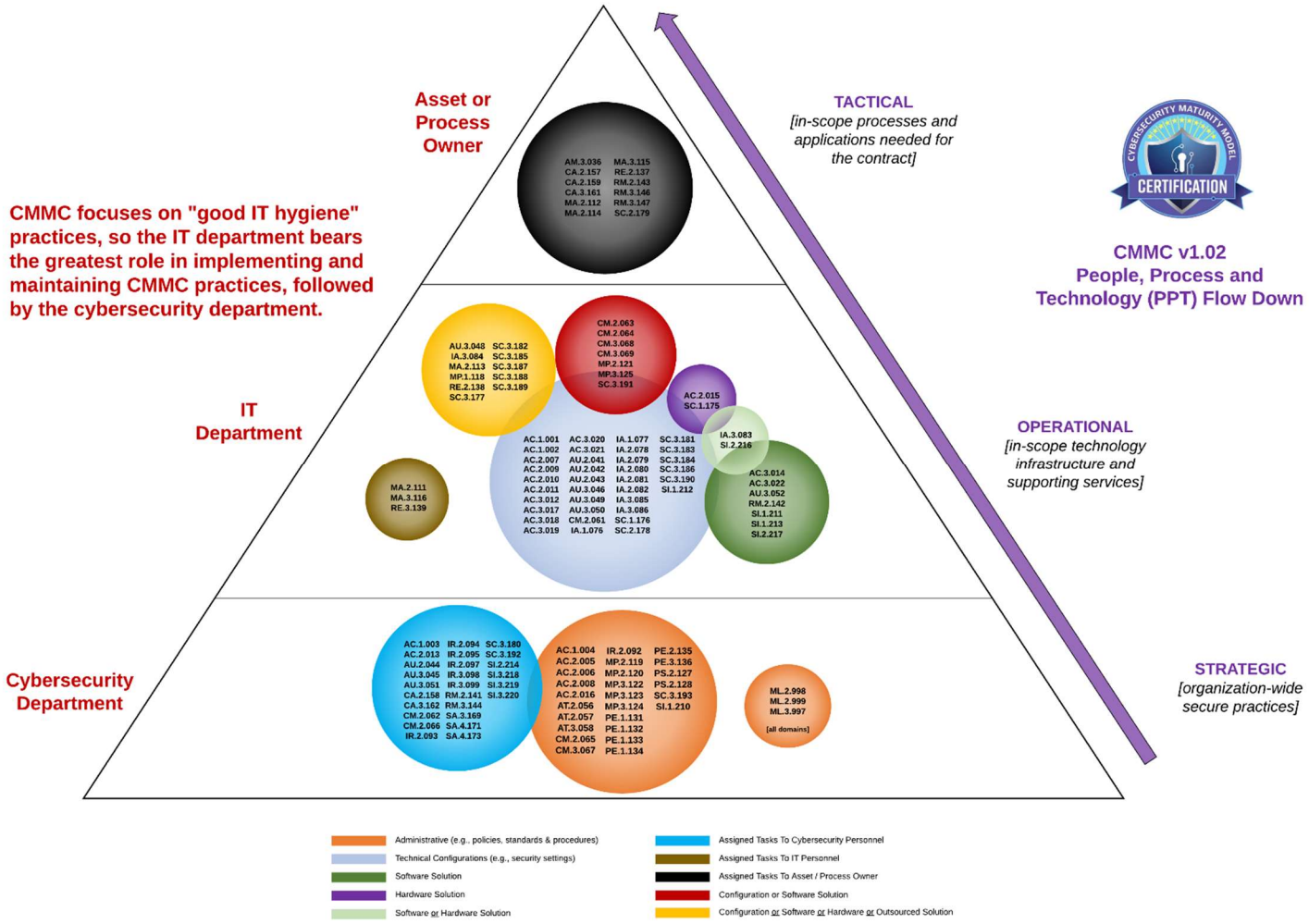
NIST 800-171 Specific Documentation

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



CONTROL / PRACTICE STAKEHOLDERS

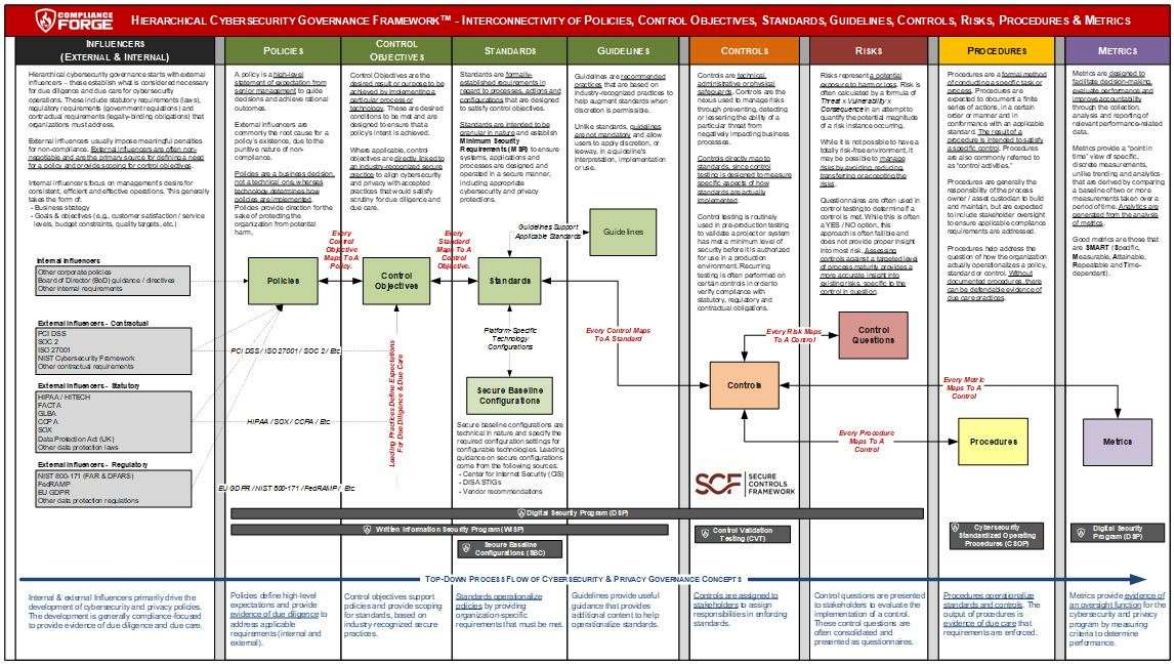
It is important for anyone getting started with NIST 800-171 / CMMC to first understand who the stakeholders are. As you can see from the diagram below, the majority of the practices/controls are "owned" by the IT department, with quite a few being the responsibility of the asset/process owner. This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



Cybersecurity Documentation Hierarchy – Understanding How Cybersecurity Documentation Is Connected

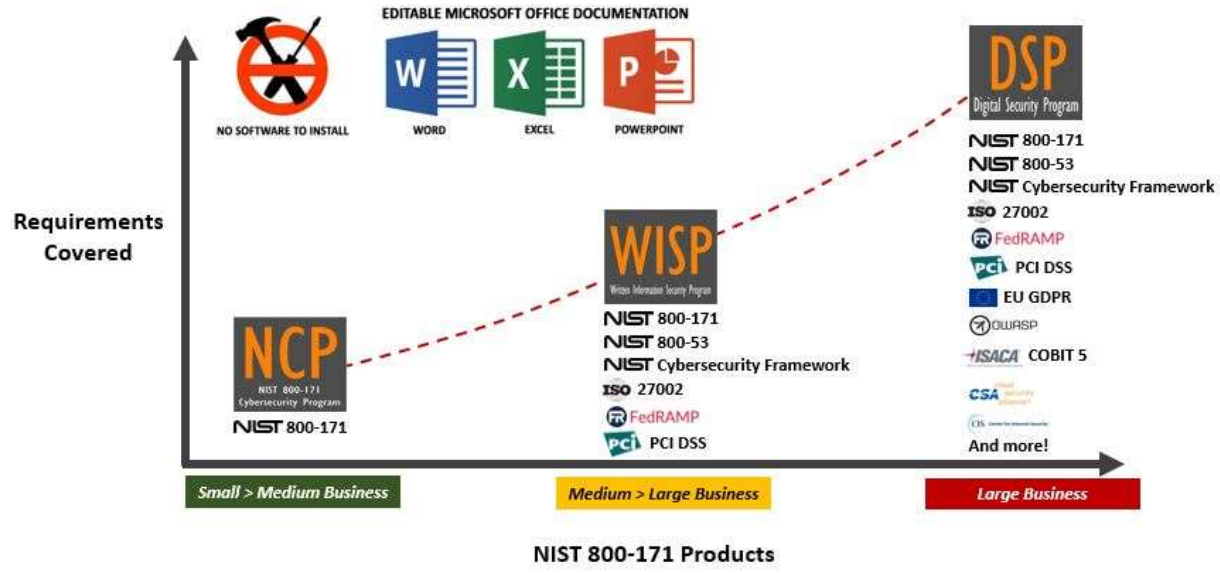
It all starts with influencers – these influencers set the tone and establish what is considered to be due care for information security operations. For external influencers, this includes statutory requirements (laws), regulatory requirements (government regulations) and contractual requirements (legally-binding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

When that is all laid out properly, your company's cybersecurity documentation show flow like this where your policies are linked all the way down to metrics:
http://examples.complianceforge.com/ComplianceForge%20Hierarchical%20Cybersecurity%20Governance%20Framework.pdf



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

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



Example NIST 800-171 Cybersecurity Documentation

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

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

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