Redspin
A Division of CynergisTek

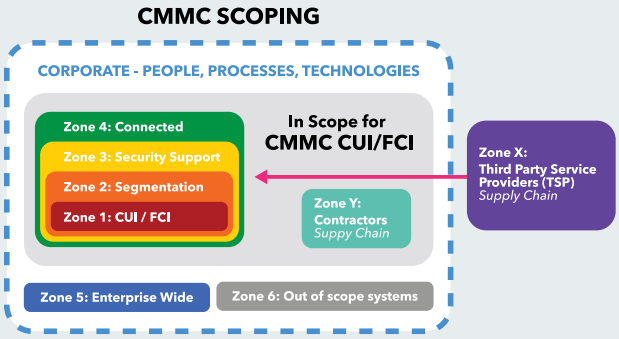
CMMC: Scoping the Environment

GETTING STARTED ON THE RIGHT FOOT

Scoping determines the boundaries where Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) is stored, processed, and exchanged within the Department of Defense (DoD) contractor's environment. If scoping is not done accurately, then the entire network and business functions may be in scope for a CMMC assessment and may be prohibitively expensive to protect the entire organization.

There is no official guidance on how to scope an environment for protection of CUI/FCI while stored, processed, and exchanged. The DoD is actively working to publish scoping guidance for CMMC assessments. The intent of this white paper is not to go into every detail for the contractor to architect its CMMC boundaries, but instead to provide a high-level overview of the foundational components that define what portions of a contractor's environment is in scope for an assessment.

Contact us for more information on scoping for your environment.



In Scope for CMMC

- Zone 1: CUI / FCI
- Zone 2: Segmentation
- Zone 3: Security Support
- Zone 4: Connected
- Zone Y: Contractors/Subcontractors

Out of Scope for CMMC

- Zone 5: Enterprise Wide
- Zone 6: Out of Scope Components

Depends

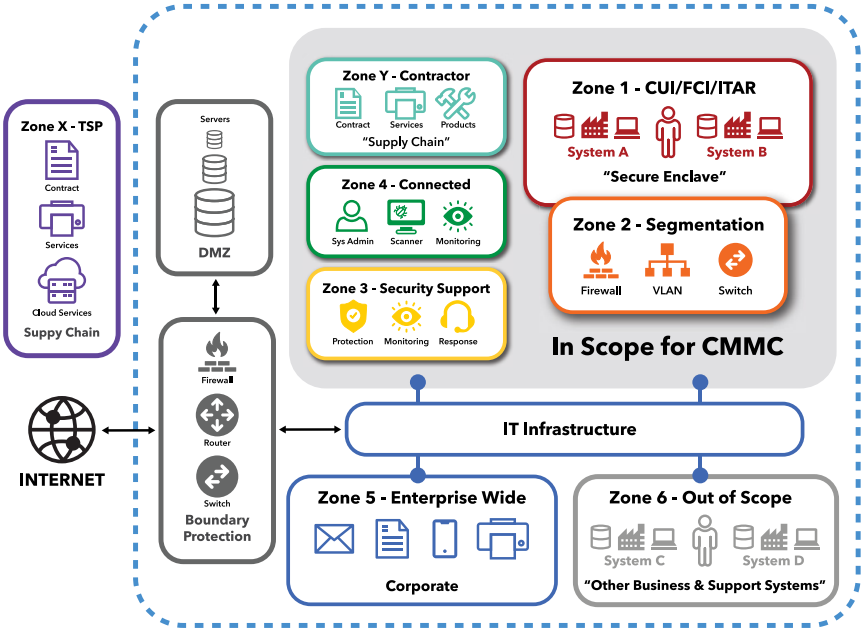
- Zone X: Third Party Service Providers

SCOPING OBJECTIVE

The overall objective of scoping is to outline the logical, physical, and functional boundaries for conducting operations to ensure that FCI/CUI data is protected at a minimum of CMMC Level 1 for FCI and CMMC Level 3 for CUI. Scoping includes documenting facilities, areas, systems, applications, and services in the organization that are within scope for NIST SP 800-171 and CMMC compliance. The intent is to isolate CUI/FCI where possible to reduce the footprint for what is in scope for a CMMC assessment for certification.

ZONES

Scoping can be viewed in eight (8) major zones as described below. The architecture for each zone will depend on the organization's size, complexity, and contractual requirements for protecting CUI/FCI. Zone 1, designated here as the "Secure Enclave," is where the storage, processing, and transmission of CUI/FCI occurs. The zones are not necessarily mutually exclusive and depend on the contractor's design and implementation of its applications, software, systems, personnel, and services and how they interact or impact the CUI/FCI within the Secure Enclave. It takes forethought and planning to architect an environment that isolates system components that store, process, or transmit FCI/CUI from systems those that do not store, process or transmit FCI/CUI.



Zone 1: CUI/FCI – Zone 1 contains the applications, software, systems, personnel, and services that directly store, process, and exchange CUI/FCI. This data must be stored and processed from within a secure enclave. Some organizations call this zone the "Secure Enclave."

Zone 2: Segmented – Zone 2 is designed to ensure that the Secure Enclave is self-contained and does not allow any access to uncontrolled areas via segmentation to logically isolate it from the rest of the organization. Properly designing and implementing segmentation will reduce the scope of a CMMC assessment.

Zone 3: Security Tools and Support – Zone 3 is designed to provide security services, people, processes, and technologies to protect, monitor, and respond to issues that may impact the Secure Enclave. Depending on the role of the security services and/or tools, this zone can be in- or out- of scope, typically dependent on access control policies. Implementation of security tools should be based on the concept of defense in depth. Managed service providers can fall into this zone.

Zone 4: Connected - Zone 4 are systems, applications, personnel, or services that have either a direct or indirect connection into the Secure Enclave. If these have the potential to impact the Secure Enclave, then they are considered to be in scope. Managed service providers can fall into this zone.

Zone 5: Enterprise Wide – Zone 5 is the organization's enterprise information security program that is required to implement and maintain the Non-Federal Organization (NFO) controls in Appendix E of NIST SP 800-171 Revision 2.

Zone 6: Out of Scope – Zone 6 are the applications, software, systems, personnel, and services that are completely isolated from the Secure Enclave. These components do not store, process, and exchange CUI/FCI and are considered out of scope.

Zone X: Third Party Service Provider – Zone X contains those contractors and subcontractors that are a part of supply chain services and must meet contractual flow-down security requirements. The role that services play will depend on if it can directly or indirectly impact the Secure Enclave.

Zone Y: Contractor / Subcontractor - Zone Y is party to the execution of the contract where the contractor is also storing, processing, and transmitting CUI/FCI. This zone is named Y due to the possibility that a contractor or its subcontractor can fall in other zones depending on its role. The contractor will always be in scope for CMMC.

Zone 2: Segmented

- Firewalls and associated configurations
- Virtualization

Zone 3: Security Support

Access Control

- Identity, Authentication, & Directory Services
- Multi-factor Authentication (MFA)
- Virtual Private Network (VPN)
- Domain Name Systems (DNS)

Monitoring, Logging, and Auditing

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Security Information Event Management (SIEM)
- Domain Name Systems (DNS)

Data Protection

- Data Loss Prevention (DLP)
- File Integrity Monitoring (FIM)

Hardware / Software / Operating System Protection

- Vulnerability & Patch Management
- Anti-virus / Anti-malware

Zone 4: Connected

- Jump Host connecting to zones in scope
- Remote Desktop Protocol (RDP)

Zone 5: Enterprise Wide

- Corporate-wide information security policies
- Enterprise network / IT infrastructure

Zone 6: Out of Scope

- Enterprise network / IT infrastructure (if segmented)
- Guest Wi-Fi (if segmented)
- Employees with no access to the Secure Enclave

Zone X: 3rd Party Service Provider (TSP)

- Contractual requirement for security documentation
- Cloud Service Provider (CSP)
- Data Storage (if includes CUI/FCI, then Zone 1)
- Data Backup (if includes CUI/FCI, then Zone 1)

Zone Y: Contractor / Subcontractor

- Contractual requirement for security documentation
- Manufacturers parts (includes CUI, then Zone 1)

Credit to: PCI Resources, ComplianceForge, and Auburn University for the underlying concept of the zone-based model to handle CUI.