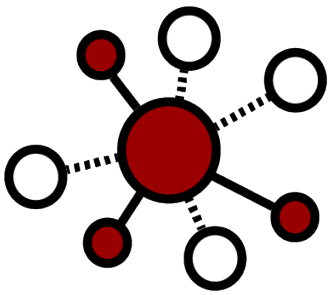
COMPLIANCE FORGE

SCF SECURE CONTROLS FRAMEWORK



Unified Scoping Guide

Sensitive & Regulated Data

Unified Scoping Guide (USG): A Zone-Based Model To Apply A Data-Centric Security Approach For Scoping Sensitive & Regulated Data*

**Applicable sensitive/regulated data types:*

- *Controlled Unclassified Information (CUI)*
- *Personally Identifiable Information (PD)*
- *Cardholder Data (CHD)*
- *Attorney-Client Privilege Information (ACPI)*
- *Export-Controlled Data (ITAR/EAR)*
- *Federal Contract Information (FCI)*
- *Protected Health Information (PHI)*
- *Intellectual Property (IP)*
- *Student Educational Records (FERPA)*
- *Critical Infrastructure Information (CII)*

Version 2025.1

Table of Contents

EXECUTIVE SUMMARY

In practical terms, cybersecurity and data protection controls exist to protect an organization's data. Requirements for asset management do not primarily exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but data residing on those devices cannot. This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity & data protection program, since it provides guidelines to establish the scope for control applicability.

This Unified Scoping Guide (USG) is intended to help organizations define the scope of the sensitive/regulated data where it is Processed, Stored and/or Transmitted (P/S/T). This guide will refer to both sensitive and regulated data as "sensitive/regulated data" to simplify the concept this document is focused on. This approach is applicable to the following sensitive/regulated data types:

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

This USG leveraged the outstanding concepts that PCI Resources published in its *PCI DSS Scoping Model and Approach*[1] and built upon that idea by applying the scoping methodology to other types of sensitive/regulated data. The USG categorizes system components according to several factors:

(1) Whether sensitive/regulated data is P/S/T;
(2) The functionality that the system component provides (e.g., access control, logging, antimalware, etc.); and
(3) The connectivity between the system and the sensitive/regulated data environment.

The model described in this document utilizes nine (9) zones to categorize system components, based on the interaction with sensitive/regulated data. This model highlights the different types of risks associated with each zone. This approach makes it evident which systems, applications and services must be appropriately protected, due to the risk posed to sensitive/regulated data. The Sensitive Data Environment (SDE) encompasses the People, Processes, Technologies, Data & Facilities (PPTDF) that P/S/T sensitive/regulated data where:

- Store means sensitive/regulated data is inactive or at rest (e.g., located on electric media, in system component memory or in physical format such as paper documents).
- Process means sensitive/regulated data is actively being used by a system component (e.g., accessed, entered, edited, manipulated, printed, viewed).
- Transmit means sensitive/regulated data is being transferred/transmitted from one asset to another asset (e.g., data in transit using physical or digital transport methods).

Secure Controls Framework Conformity Assessment Program (SCF CAP)

The Secure Controls Framework (SCF) designated the USG as the official scoping guidance for the SCF's Conformity Assessment Program (SCF CAP).[2] The SCF CAP is designed to conduct Third Party Assessment, Attestation and Certification Services (3PAAC Services), so clear and concise scoping guidance is a necessity to designate cybersecurity and/or data protection controls as being in or out of scope.

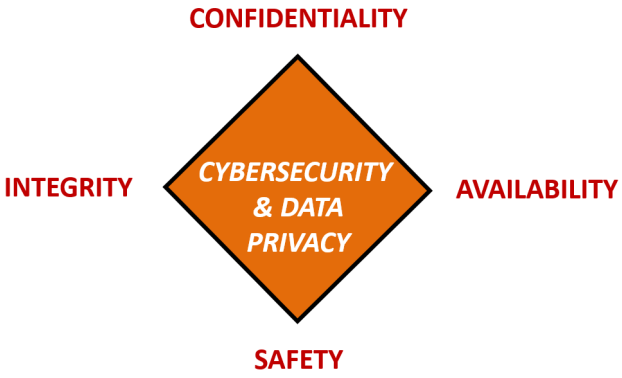
Due Diligence

Failure to adequately perform due diligence in scoping activities may lead to every system, application and service in your organization to be considered in scope and require applicable statutory, regulatory and/or contractual controls.

[1] *PCI Resources - PCI DSS Scoping Model and Approach* https://www.pciresources.com/pci-dss-scoping-model-and-approach/
[2] *SCF Conformity Assessment Program (SCF CAP) -* https://securecontrolsframework.com/scf-conformity-assessment-program-cap/

UNDERSTANDING THE INTENT OF SCOPING SENSITIVE DATA

Protecting data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security and data privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- *CONFIDENTIALITY* addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- *INTEGRITY* addresses guarding against improper modification or destruction, including ensuring non-repudiation and authenticity.
- *AVAILABILITY* addresses timely, reliable access to data, systems and services for authorized users.
- *SAFETY* addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

SCOPING ≠ APPLICABILITY

Control scoping does not mean all controls apply uniformly to every person, process, technology, type of data or facility. This misunderstanding of applicability vs scoping is one of the biggest hurdles that organizations face, since there is a common misconception that if something is "in scope" then every control will be applicable across the entire boundary of the assessment. This is an incorrect assumption. When you look at the breath of controls that an organization is obligated to comply with, the controls are often administrative, technical or physical, in nature. This means that there may be controls that are not applicable to certain systems, applications and/or processes.

Example 1: Network firewall

- A network firewall is a technical control, where certain other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- Since a network firewall is a device, it not capable of having end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.

Example 2: User awareness training

- User awareness training is focused on personnel, such as employees and applicable third-parties who will be interacting with the organization's systems and data. NDAs, threat intelligence awareness, acceptable use notifications are all applicable to individuals.
- Since an individual is not a device, an individual is not capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.

Example 3: Incident Response Plan (IRP)

- An IRP is a documented process that is a tool to be used to guide incident response operations.
- Since an IRP is a not an individual or technology, it cannot sign an NDA, have MFA or be patched.

The best solution is to create some form of a matrix that can apply the appropriate controls to the correct PPTDF to help identify the correct scope for the implementation of controls.

RATIONALIZING DATA SCOPING RECOMMENDATIONS

There are two (2) main sources of guidance for scoping activities:

1. Payment Card Industry Data Security Standard (PCI DSS); and
2. 32 CFR Part 170 - Cybersecurity Maturity Model Certification (CMMC) Program

This guide leveraged the outstanding concepts that PCI Resources published in its PCI DSS Scoping Model and Approach[3] by applying that scoping methodology to other types of sensitive/regulated data, including but not limited to:

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

This model categorizes system components according to several factors:

- Whether sensitive/regulated data is being P/S/T;
- The functionality that the system component provides (e.g., access control, logging, antimalware, etc.); and
- The connectivity between the system and the sensitive/regulated data environment.

PCI DSS SCOPING CONSIDERATIONS:

For non-DoD-related scoping considerations, PCI DSS generally reigns, due to its long-established and internationally-recognized practices for protecting cardholder data (e.g., credit and debit cards). PCI DSS v1.0 was first published in 2004, so it has twenty (20) years of guidance for "what looks right" to scope environments that require the implementation of PCI DSS controls to protect the confidentiality and integrity of cardholder data. The Payment Card Industry Security Standards Council (PCI SSC) publishes an authoritative scoping guide for merchants to leverage for PCI DSS compliance efforts.[4] This PCI SSC scoping guidance is based on real-world threats and practical lessons-learned on how segmentation can be used to minimize scoping, due to limiting the ability of threats to negatively impact cardholder data.

PCI DSS is a well-established and widely adopted standard for protecting cardholder data (e.g., credit and debit cards). From the perspective of PCI DSS, if scoping is done poorly, an organization's entire network may be in-scope, which means PCI DSS requirements would apply uniformly throughout the entire company's network. 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 Cardholder Data Environment (CDE) can be a small fraction of the company's network, which makes compliance much more achievable and affordable.

When you look at sensitive/regulated data compliance scoping, it has some similarities to PCI DSS:

- PCI DSS is focused on protecting the confidentiality and integrity of cardholder data, which is where credit/debit card data is P/S/T.
- Statutory, regulatory and contractual obligations to protect sensitive/regulated data require controls to be implemented on the applicable environment(s) (e.g., system, application, service, etc.) where the sensitive/regulated data is P/S/T. This is how PCI DSS applies its controls from a scoping perspective.
- Cardholder data is considered "infectious" from the perspective of scoping. Without proper segmentation and clear business processes, other forms of sensitive/regulated data can "infect" the entire network and greatly expand the scope of compliance and audits.

---

[3] *PCI Resources - PCI DSS Scoping Model and Approach https://www.pciresources.com/pci-dss-scoping-model-and-approach/*
[4] *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation - https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf*

32 CFR Part 170/CMMC Scoping Considerations

32 CFR Part 170 does not change the five (5) existing categories of assets within CMMC:[5]

1. CUI Assets;
2. Security Protection Assets (SPA);
3. Contractor Risk Managed Assets (CRMA);
4. Specialized Assets (SA); and
5. Out-of-Scope Assets (OOSA).

What 32 CFR Part 170 does is provide some clarification on scoping:

- CRMA should be prepared to be assessed against applicable CMMC requirements, subject to the assessor's discretion.
- SA need to be documented, but are not assessed using CMMC requirements.
- Cloud Service Providers (CSP) must meet the requirements of the FedRAMP moderate baseline in accordance with DFARS clause 252.204-7012(b)(2)(ii)(D).
- External Service Provider (ESP)
    - Do not require CMMC assessment or certification if the ESP:
        - Only stores Security Protected Data (SPD);
        - Provides a Security Protection Assets (SPA); and/or
        - Does not P/S/T CUI.
    - Services are assessed as SPA.

Differences Between PCI DSS and 32 CFR Part 170/CMMC Scoping Guidance

The depth of scope is the key difference between these competing concepts for how to scope an assessment boundary. Somewhat surprisingly, the differences are primarily how PCI DSS more aggressively protects payment card data than the US Department of Defense (DoD) protects CUI. Examples include:

- Virtual Desktop Infrastructure (VDI) is in-scope for PCI DSS, but not CMMC; and
- CMMC creates categories of assets to remove them from scope, where those assets would be in scope for PCI DSS (e.g., Contractor Risk Managed Assets (CRMA) and Specialized Assets (SA)).

What This Guide Does Address

Identifying and addressing the People, Processes, Technologies, Data & Facilities (PPTDF) around sensitive/regulated data is a necessary part of any cybersecurity and data protection (data privacy) 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 an assessor/regulator by providing a reasonable methodology to describe your technology infrastructure and sensitive/regulated data 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 sensitive/regulated data by re-architecting technologies to isolate and control access to the sensitive/regulated data environment.

This model categorizes system components according to several factors:

- Whether sensitive/regulated data is being P/S/T;
- The functionality that the system component provides (e.g., access control, logging, antimalware, etc.); and
- The connectivity between the system and the Sensitive Data Environment (SDE).

What This Guide Does Not Address

This guide does not define which statutory, regulatory and/or contractual controls are required for each category. Since every organization is different, it is up to each organization and its assessor to determine the nature, extent and effectiveness of each control to adequately mitigate the risks to sensitive/regulated data.

[5] *DoD CIO CMMC Resources & Documentation - https://dodcio.defense.gov/CMMC/Resources-Documentation/*

SEGMENTATION CONSIDERATIONS

It is important to understand that without adequate network segmentation (e.g., a flat network) the entire network would be expected to be in scope for an assessment. Network segmentation should be viewed as a very beneficial process to isolate system components that P/S/T sensitive/regulated data from systems that do not. Adequate network segmentation may reduce the scope of the SDE and overall reduce the scope of an assessment. It is important to point out that Zero Trust Architecture (ZTA) still has scoping requirements and is not a "magic bullet" to eliminate scoping requirements. Examples of mechanisms that provide controlled access include firewalls, routers, hypervisors, micro-segmentation (e.g., ZTA), etc.

To eliminate ambiguity surrounding the term "segmentation" in terms of sensitive/regulated data enclave scoping, this guide uses one of the two following terms:

- **Isolation** – No logical access. This is achieved when network traffic between two (2), or more, 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; and
  - 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.

TERMINOLOGY & ACRONYMS

The USG defaults to three (3) primary sources for authoritative definitions for cybersecurity and data privacy terminology:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[6] and
- NIST Glossary;[7] and
- 32 CFR Part 170.[8]

From the context of applying statutory, regulatory and/or contractual requirements to scoping decisions, it is important to clarify mandatory versus optional criteria:[9]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

TERMINOLOGY STANDARDIZATION

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an organization's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire organization;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an organization; or
    - A specific country, or geographic region, of the organization's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Compensating Control. If a required control cannot be implemented due to legitimate technical, financial or other business constraints, a compensating control is an alternative safeguard, or countermeasure, that is employed in lieu of the control that cannot be met.
- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. [10]
- Enclave. This is a distinct set of assets that operate in the same security domain and share the protection of a single, common, continuous security perimeter. The SDE can be an enclave within your organization's broader corporate network.
- Implemented Capability. An implemented capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.
- Reciprocity. Reciprocity is an agreement among participating organizations to accept each other's: [11]

---

[6] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[7] *NIST Glossary - https://csrc.nist.gov/glossary*
[8] *32 CFR Part 170(b) - https://www.federalregister.gov/d/2024-22905/p-1951*
[9] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*
[10] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*
[11] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*

- Security assessments to reuse system resources; and/or
- Assessed security posture to share information.

- Security Control. Security controls are administrative, physical and technical in nature. These controls are safeguards, or countermeasures, prescribed for in-scope systems, applications, services, organizations, etc. to protect the Confidentiality, Integrity, Availability and Safety (CIAS) of an organization's data and systems.

ACRONYMS

The following acronyms are used throughout the CDPAS:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations (e.g., internal assessments).
3PA	Third-Party Attestation	3PA are attestations made by an independent third-party, generally in the performance of an assessment or audit.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
CSP	Cloud Service Provider	CSP refers to an external company that provides cloud services based on cloud computing. An External Service Provider (ESP) providing cloud computing services is a CSP. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145. This cloud model is composed of five (5) essential characteristics, three (3) service models, and four (4) deployment models.[12] Essential Characteristics: 1. On-demand self-service; 2. Broad network access; 3. Resource pooling; 4. Rapid elasticity; and 5. Measured service. Service Models: 1. Software as a Service (SaaS); 2. Platform as a Service (PaaS); and 3. Infrastructure as a Service (IaaS). Deployment Models: 1. Private cloud; 2. Community cloud; 3. Public cloud; and 4. Hybrid cloud.
ESP	External Service Provider	An independent, third-party organization that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting/professional services; ▪ Software development; ▪ Staff augmentation; and

[12] *32 CFR Part 170 & NIST SP 800-145 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*

		▪ Technology support (e.g., Managed Services Provider (MSP)).
OSA	Organization Seeking Assessment	A company, entity or business unit seeking the external assessment. An OSA is an entity seeking to conduct, obtain, or maintain an assessment. The term OSA includes all OSCs.
OSC	Organization Seeking Certification	An OSC is an entity seeking to contract, obtain, or maintain certification. An OSC is also an OSA.
PPTDF	People, Processes, Technologies, Data & Facilities	Five (5) components that provide a lens to view the applicability of controls: ▪ People - Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.). ▪ Processes - Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.). ▪ Technologies - Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.). ▪ Data - Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.). ▪ Facilities - Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
P/S/T	Store, Process and/or Transmit	Refers to storing, processing and/or transmitting sensitive/regulated data where: ▪ Store means sensitive/regulated data is inactive or at rest (e.g., located on electric media, in system component memory or in physical format such as paper documents). ▪ Process means sensitive/regulated data is actively being used by a system component (e.g., accessed, entered, edited, manipulated, printed, viewed). ▪ Transmit means sensitive/regulated data is being transferred/transmitted from one asset to another asset (e.g., data in transit using physical or digital transport methods).
SPD	Security Protection Data	SPD refers to security-relevant data that includes, but is not limited to: ▪ Configuration data; ▪ Event log files; ▪ Vulnerability data; and ▪ Authenticators (e.g., passwords).

PERSPECTIVE: VIEW SENSITIVE & REGULATED SCOPING FROM A SPILLAGE EVENT

A "data spill" is a security incident that results in the transfer of sensitive or regulated data onto a system, application or processes that is not authorized to P/S/T that type of data. The justification for the time and effort spent going through a scoping exercise is to avoid a spillage event.

DATA SPILLAGE PREVENTION CONSIDERATIONS

The government of Australia publishes a data spill management guide that is a worthwhile reference for any form of sensitive/regulated data spillage.[13] The key step is to "appropriately identify and handle information" since that can greatly assist in preventing data spills. This comes down to having appropriate scoping for sensitive/regulated data so that the necessary controls can be applied.

In the event of a data spill, organizations are encouraged to use the following five (5) step process:

1. Identify. Recognize that a data spill has taken place.
2. Contain. Determine the breadth of the data spill.
3. Assess. Decide on the most appropriate course of action to address the data spill.
4. Remediate. Remediate the data spill based on the course of action chosen.
5. Prevent. Implement prevention measures to stop similar incidents from occurring in the future.

The ability to respond to a data spill fundamentally requires that the organization knows where the data should and should not be, which brings scoping into the discussion. Response to data spills require the organization to:

- Track data flow, movement and storage locations of the spilled data to assist in determining what devices and systems are affected; and
- Identify affected system users, including any external to the organization.

While the identification process highlights the systems and users that are initially affected, a more thorough assessment should be performed after the containment process. This includes devices such as workstations, backup storage, printers, print servers, network shares, email inbox and servers, content filtering appliances, webmail and external systems.

While covering classified information, National Industrial Security Program Operating Manual (NISPOM)[14] contains guidance for US government contractors on maintaining an information security program that supports overall information security by incorporating a risk-based set of administrative, physical and technical security controls in accordance with agency-provided guidance to incorporate the following aspects into the organization's information security program:

- Policies and procedures that reduce information security risks to an acceptable level and address information security throughout the information system life cycle.
- Plans and procedures to assess, report, isolate, and contain data spills and compromises, to include sanitization and recovery methods.

DATA SPILLAGE RESPONSE CONSIDERATIONS

NIST SP 800-53 R5 contains a control on "information spillage response" that an organization should reference as a guideline to view how its scoping activities support or hurt its ability to appropriately respond to a data spill of sensitive or regulated data. If your organization's scoping efforts does not *adequately* support this control, then your organization should re-evaluate its scoping efforts and existing controls.

> **IR-9 INFORMATION SPILLAGE RESPONSE**[15]
> Control: Respond to information spills by:
> a. Assigning *[Assignment: organization-defined personnel or roles]* with responsibility for responding to information

[13] *Australia Data Spill Management Guide* - https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Data%20Spill%20Management%20Guide%20%28June%202020%29.pdf
[14] *NISPOM* - https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom
[15] *NIST SP 800-53 R5* - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

spills;
b. Identifying the specific information involved in the system contamination;
c. Alerting *[Assignment: organization-defined personnel or roles]* of the information spill using a method of communication not associated with the spill;
d. Isolating the contaminated system or system component;
e. Eradicating the information from the contaminated system or component;
f. Identifying other systems or system components that may have been subsequently contaminated; and
g. Performing the following additional actions: *[Assignment: organization-defined actions]*.

Discussion: Information spillage refers to instances where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. At that point, corrective action is required. The nature of the response is based on the classification or impact level of the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The methods used to communicate information about the spill after the fact do not involve methods directly associated with the actual spill to minimize the risk of further spreading the contamination before such contamination is isolated and eradicated.

Defining Control Applicability: Administrative, Physical & Technical Control Scoping

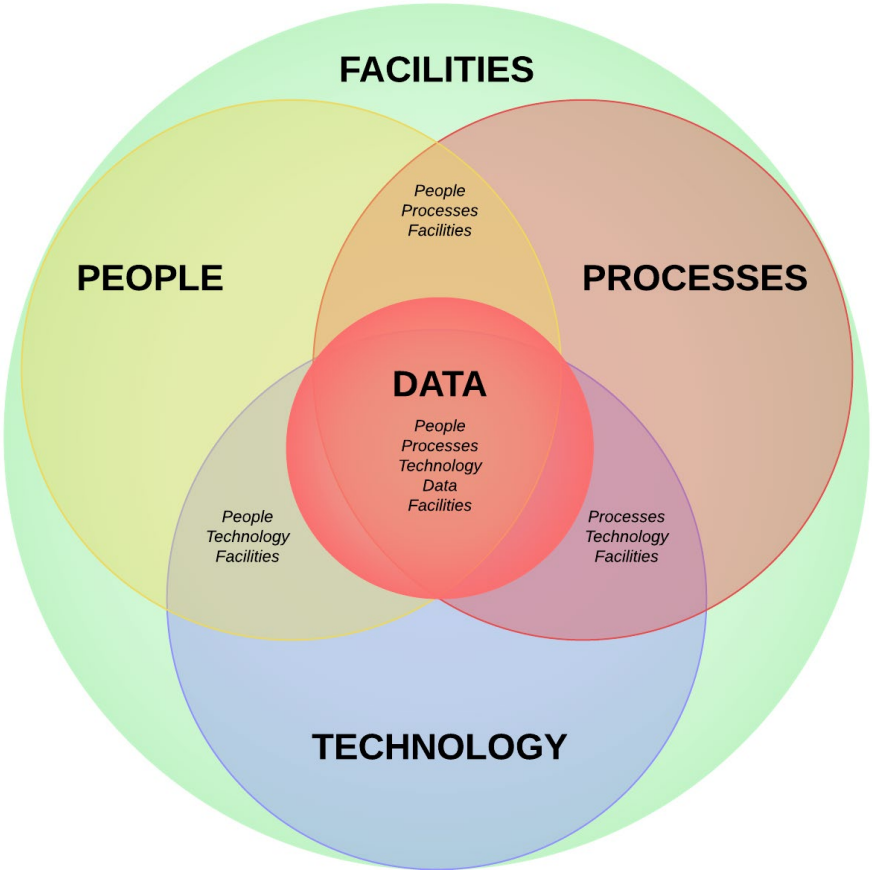
There are two (2) aspects of scoping that need to be clarified:

1. Defining the assessment boundary that identifies the People, Processes, Technologies, Data & Facilities (PPTDF) that are in-scope; and
2. Defining what controls are applicable for the in-scope PPTDF.

People, Processes, Technologies, Data & Facilities (PPTDF)

The PPTDF model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls.

1. People - Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
2. Processes - Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
3. Technologies - Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.).
4. Data - Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
5. Facilities - Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



Assessment Boundary (Macro Scoping)

The assessment boundary is the "security perimeter" that defines what is in-scope or out-of-scope for systems, applications, services, etc. The assessment boundary defines not just the Sensitive Data Environment (SDE), but the PPTDF that influence the security of the SDE, which would also require applicable security controls.

The assessment boundary may be a simple SDE enclave, which is a distinct set of assets that operate in the same security domain and share the protection of a single, common, continuous security perimeter. The SDE enclave can exist within your organization's broader corporate network, just like other network segmentations such as a Demilitarized Zone (DMZ). The assessment boundary may also be a more complex arrangement of on-premises, cloud-based and other third-parties. The zone-based approach to implementing data-centric security protections described in this scoping guide is meant to help define the assessment boundary, regardless of its complexity.

Control Applicability for People, Processes, Technology, Data & Facilities (Micro Scoping)

Security controls are safeguards or countermeasures prescribed for in-scope PPTDF to protect the confidentiality, integrity, availability and safety of its information and to meet a set of defined security requirements. If a required control cannot be implemented due to legitimate technical, financial or other business constraints, a compensating control is often a viable, alternative safeguard or countermeasure that can be employed in lieu of the control that cannot be met.

Without clear guidance from a statutory or regulatory body on control applicability within the assessment boundary, it becomes a subjective exercise. This subjectivity is the reason clear documentation is needed to provide evidence of the rationalization that went into making a control applicability decision. Controls are commonly categorized as belonging to one of these three (3) functions:

1. Administrative;
2. Physical; or
3. Technical.

Administrative

- Administrative controls are non-technical mechanisms that define and guide employee actions in dealing with cybersecurity & data privacy topics.
- Examples of administrative controls include, but are not limited to:
  - Policies;
  - Standards;
  - Metrics;
  - Security program governance;
  - Risk management; and
  - Procurement/supply chain.

Physical

- Physical controls are primarily focused on restricting physical access to an organization's PPTDF.
- Examples of physical controls include, but are not limited to:
  - Employee badges;
  - Visitor control;
  - Video surveillance;
  - Burglar alarms;
  - Doors;
  - Locks;
  - Fences;
  - Proximity badges; and
  - Security guards.

Technical

- Technical controls are primarily technical in nature. These are devices, applications, processes, protocols and other technical measures, are used to protect the Confidentiality, Integrity, Availability and Safety (CIAS) of an organization's technology assets and data.
- Technical controls are often dependent upon the proper functioning of the system for their effectiveness and therefore require significant operational considerations.
- Examples of technical controls include, but are not limited to:
  - Antimalware;
  - Firewalls;

- Log management (e.g., SIEM);
- Intrusion Prevention System (IPS);
- DNS filtering; and
- Encryption.

STEPS TO DEFINE "APPLICABLE CONTROLS"

The process for distilling control applicability should follow the methodology described below:

1. Conduct appropriate due diligence steps to define the business process(es) and the associated PPTDF that make up the assessment boundary:
    a. Document a System Security Plan (SSP), or similar document, to clearly identify the PPTDF that influence the security of the SDE.
    b. Document and keep current an inventory of all PEOPLE (or groups of people) who operate with the Secure Data Environment (SDE) and who influence the security of the SDE. That includes, but is not limited to:
        i. Line of Business (LOB) stakeholders;
        ii. IT/cybersecurity leadership;
        iii. Business operations stakeholders (e.g., HR, physical security, etc.);
        iv. End users;
        v. Cybersecurity practitioners (e.g., analysts, engineers, architects, consultants, etc.);
        vi. Cloud Service Provider (CSPs);
        vii. Managed Service Providers (MSPs);
        viii. Managed Service Security Providers (MSSPs);
        ix. External Service Providers (ESP); and
        x. Contractors/sub-contractors.
    c. Document and keep current an inventory of all **TECHNOLOGIES** that are within the SDE and influence the security of the SDE that includes, but is not limited to:
        i. Servers;
        ii. Workstations;
        iii. Network devices;
        iv. Mobile devices;
        v. Databases;
        vi. External Service Providers (ESP);
        vii. Cloud instances:
            1. Private clouds;
            2. Community clouds;
            3. Public clouds; and
            4. Hybrid clouds;
        viii. Major applications (including what servers and databases they depend on).
        ix. Minor applications (e.g., electronic messaging systems, Internet browsers, productivity suites, etc.).
    d. Document and keep current an inventory of all **PROCESSES** that intake, process, maintain, distribute, sanitize and/or dispose of sensitive/regulated data that includes, but is not limited to:
        i. Electronic messaging systems (e.g., email, instant messaging, SMS, wiki, etc.);
        ii. Application Program Interfaces (APIs);
        iii. Enterprise Resource Management (ERM);
        iv. Enterprise Resource Planning (ERP);
        v. Customer Resource Management (CRM);
        vi. Governance, Risk Management & Compliance (GRC);
        vii. Workflow/ticket management (e.g., JIRA, ServiceNow, etc.); and
        viii. Collaboration technologies (e.g., SharePoint).
    e. 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:
        i. A high-level diagram can be "cartoonish" to depict broad concepts.
        ii. A low-level diagram needs to be detailed and identify the ports, protocols and services that are used across the SDE. This information should match what exists in applicable Access Control Lists (ACLs).
        iii. A Data Flow Diagram (DFD) that maps the flow of all sensitive/regulated data between:
            1. Organizations (e.g., sharing information between organizations);

    2. Business processes (e.g., how the information is meant to be shared internal to an organization); and
    3. Systems/applications/services (e.g., system interconnections to make a process function).
2. If your control set is not already designated, identify the function of each control (e.g., administrative, physical or technical):
    a. Administrative controls are non-technical measures (e.g., policies, standards, procedures, SSP, IRP and other documents);
    b. Physical controls may have technical components, but are focused on restricting physical access (e.g., doors, locks, fences, proximity badges, visitor control, etc.); and
    c. Technical are implemented to ensure conformance with a requirement (e.g., secure configuration builds, antimalware software, intrusion detection, event logging, etc.)
3. For **PEOPLE** who work within the assessment boundary:
    a. Identify the stakeholder(s) who "own" the controls;
    b. Identify the individual contributor(s) (or roles) who operate the controls; and
    c. Assign all administrative and physical controls to those appropriate stakeholders and individual contributors.
4. For **PROCESSES** that exist within the assessment boundary:
    a. From the DFD and network diagrams, identify the processes that require controls to be applied; and
    b. Assign all applicable administrative, physical and technical controls to the process(es).
5. For **TECHNOLOGIES** that exists within the assessment boundary:
    a. Identify all the technology solutions (e.g., systems, applications & services); and
    b. Assign all applicable technical controls to each technology solution.
6. For **DATA** that exists within the assessment boundary:
    a. Identify all the systems, applications and services where the data is P/S/T; and
    b. Ensure those systems, applications and services have the appropriate technical controls implemented.
7. For **FACILITIES** that exist within the assessment boundary:
    a. Identify all facilities where the data is P/S/T; and
    b. Ensure those facilities have the appropriate administrative, physical and technical controls implemented.

DATA TYPE CONSIDERATIONS

The reality of security and data protection controls is that control implementation equates to an incurred cost by an organization, so it makes financial sense for organizations to understand where controls must be implemented to avoid "blanket coverage" for implementing controls that could be cost-prohibitive. Scoping should be considered a fiduciary responsibility.

This document refers to both sensitive and regulated data as "sensitive/regulated data" to simplify terminology. The concept of sensitive/regulated data is applicable to the following data types:

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

US GOVERNMENT DATA CLASSIFICATIONS

Executive Orders (EO) 12356 and 13526 established the foundation for what "classified" data is. EO 13556 established the foundation for Controlled Unclassified Information (CUI).[16]

CLASSIFICATION	UNCLASSIFIED					CLASSIFIED		
TYPE	UNCONTROLLED UNCLASSIFIED INFORMATION (UUI)			CONTROLLED UNCLASSIFIED INFORMATION (CUI)		CONFIDENTIAL	SECRET	TOP SECRET
SUB-TYPE	PUBLIC RELEASE*	FCI	UUI	CUI BASIC	CUI SPECIFIED			
DEFINITION	* The US Government does not have a "PUBLIC RELEASE" designation for information. This is information that is UUI, but not FCI or CUI designated. Per NARA, UUI is subject to agency-specific "public release policies" so it is information that has undergone a public release review process.	Federal Contract Information (FCI) is not intended for public release. It is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.	Uncontrolled Unclassified Information (UUI) is information that is neither defined in EO 13556, nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.	A subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.	A subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements.	Applied to information that the unauthorized disclosure of could reasonably be expected to cause damage to the national security.	Applied to information that the unauthorized disclosure could reasonably be expected to cause serious damage to the national security.	Applied to information that the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.
PORTION MARKING	(U)	(U)	(U)	(CUI)	(CUI//SP-XX)	(C)	(S)	(TS)
CLEARANCE REQUIREMENTS	NONE - No US Government-issued clearance requirements exist for UUI or CUI					Confidential Clearance	Secret Clearance	Top Secret Clearance
SUPERSEDES / REPLACES	N/A			For Official Use Only (FOUO) Sensitive but Unclassified (SBU)		N/A		
EXPORT CONTROLS	Not Export Controlled			ITAR / EAR IMPLICATIONS (US STATE DEPARTMENT EXPORT CONTROLS)				
DEFINITION AUTHORITY	EO 13526 / EO 13556	FAR 52.204-21	UNDEFINED	EO 13556 / US NATIONAL ARCHIVES (NARA)		EO 12356 / EO 13526		

There are two (2) types of Unclassified data from the US Government's perspective:

1. Controlled Unclassified Information (CUI) that is further broken down into:
    a. CUI Basic
    b. CUI Specified
2. Uncontrolled Unclassified Information (UUI) that is further broken down into:
    a. General UUI (not publicly released or FCI)
    b. Federal Contract Information (FCI)
    c. Information that has been cleared for public release

There are three (3) types of Classified data from the US Government's perspective:

1. Confidential;
2. Secret; and
3. Top Secret.

[16] *Classified vs Unclassified Data Types - https://complianceforge.com/nist-800-171/unclassified-vs-classified-uui-vs-cui-vs-confidential-vs-secret-vs-top-secret*

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

If you are unsure what CUI data is, you are highly-encouraged to visit the US government's authoritative source on CUI, the US Archive's CUI Registry.[17] However, to help prevent making everything CUI, per Section 3(b) of Executive Order 13556, "if there is significant doubt about whether information should be designated as CUI, it shall not be so designated."

The CMMC 2.0 Department of Defense Scoping Guidance section of this guide takes the DoD's current Cybersecurity Maturity Model Certification (CMMC)-specific scoping guidance into account as it applies to this scoping model.

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.[18] This DFARS clause requires compliance with NIST SP 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 P/S/T "Covered Defense Information."
- Covered Defense Information (CDI) means unclassified "Controlled Technical Information" or other information, as described in sensitive/regulated data 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.

NIST SP 800-171 requires private companies to protect the confidentiality of CUI where it is P/S/T. The CUI requirements within NIST SP 800-171 are directly linked to NIST SP 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.

For the Defense Industrial Base (DIB), on top of NIST SP 800-171 controls, DFARS 252.204-7021 requires defense contractors to also obtain certification with CMMC. [19]

FEDERAL CONTRACT INFORMATION (FCI)

FCI is a *very broad* data classification category. Federal Acquisition Regulation (FAR) 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, lists fifteen (15) cybersecurity requirements.[20] These requirements form the basis of Cybersecurity Maturity Model Certification (CMMC) Level 1 practices.

Per FAR 52.204-21, FCI is defined as "*information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.*"

FCI includes any communication or representation of knowledge such as:

- Facts;
- Data; and
- Opinions.

---

[17] *US National Archives CUI Registry - https://www.archives.gov/cui*
[18] *DFARS 252.204-7012 - https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting*
[19] *DFARS 252.204-7021 - https://www.acquisition.gov/dfars/252.204-7021-cybersecurity-maturity-model-certification-requirements*
[20] *FAR 52.204-21 - https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems*

FCI can be in any medium or form, including:

- Textual;
- Numerical;
- Graphic;
- Cartographic;
- Narrative; or
- Audiovisual.

PERSONAL DATA (PD)

The concept of "personally identifiable information" is nebulous, due to conflicting definitions from various laws, regulations and frameworks. The key concept to keep in mind is that not all PD is sensitive, such as an individual's name in conjunction with a photo, which can be found on sources that range from social networking sites to identification cards. When an individual's name is tied to other relevant information that could lead to criminal activity (e.g., identity theft, stalking, kidnapping, etc.) or discrimination, that is when the information becomes sensitive/regulated data.

In the examples below, various definitions of PD are shown to demonstrate the significant differences between authoritative sources, so it is the responsibility of every organization to conduct appropriate due diligence to establish the context for what PD is specific to the organization's unique business case:

US – FEDERAL GOVERNMENT (OMB)

Per the US Government's Office of Management and Budget (OMB) Memorandum M-07-16, PD is defined as "*information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.*"

US – FEDERAL GOVERNMENT (NARA)

Per the US National Archives (NARA), "sensitive PD" is defined as "*A subset of PD that, if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual*." Some forms of PD are sensitive as stand-alone elements.

a. Examples of stand-alone PD include Social Security Numbers (SSN), driver's licenses or state identification numbers; Alien Registration Numbers; financial account numbers; and biometric identifiers such as fingerprint, voiceprint, or iris scans.
b. Additional examples of SPD include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:
    - Truncated SSN (such as last four digits);
    - Date of birth (month, day, and year);
    - Citizenship or immigration status;
    - Ethnic or religious affiliation;
    - Sexual orientation;
    - Criminal history;
    - Medical information; and
    - System authentication information such as mother's maiden name, account passwords, or personal identification numbers.
c. Other PD may be "sensitive" depending on its context, such as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PD but is not sensitive.

Note: Per NARA's CUI Program, Sensitive PD is considered CUI[21]

US – STATE GOVERNMENT

The California Consumer Privacy Act (CCPA)/Consumer Privacy Rights Act (CPRA) leverages CA Civil Code 1798.81.5 to identify instances where reasonable security practices must exist to protect sensitive personal information from unauthorized access,

[21] *NARA Sensitive PD - https://www.archives.gov/cui/registry/category-detail/sensitive-personally-identifiable-info*

destruction, use, modification, or disclosure.[22] While 1798.81.5 refers to this as "personal information" the CCPA definitions are targeted towards "sensitive personally identifiable information" where the 1798.81.5 definition includes:

- An individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:
  - Social security number.
  - Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
  - Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
  - Medical information.
  - Health insurance information.
  - Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes.
- A username or email address in combination with a password or security question and answer that would permit access to an online account.

European Union (EU)

Article 4, Section 1 of the EU General Data Protection Regulation (GDPR) defines "personal data" as:

- Any information relating to an identified or identifiable natural person ('data subject');
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:
  - A name;
  - An identification number;
  - Location data;
  - An online identifier; or
  - To one or more factors specific to the:
    - Physical;
    - Physiological;
    - Genetic;
    - Mental;
    - Economic;
    - Cultural; or
    - Social identity of that natural person.

Protected Health Information (PHI)

Per 45 CFR § 160.103, PHI is defined as individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   i. Transmitted by electronic media;
   ii. Maintained in electronic media; or
   iii. Transmitted or maintained in any other form or medium.
2. Protected health information excludes individually identifiable health information:
   i. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
   ii. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
   iii. In employment records held by a covered entity in its role as employer; and
   iv. Regarding a person who has been deceased for more than 50 years.

Cardholder Data (CHD)

Per the PCI Security Standards Council, CHD is defined (at a minimum) as the full Primary Account Number (PAN). CHD may also appear in the form of the full PAN plus any sensitive authentication data, including:

[22] *CA Civil Code 1798.81.5* - https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5

- Cardholder name; and
- Expiration date and/or service code.

Intellectual Property (IP)

Not all IP is equally valued by organizations, so it is important for organizations to develop a data classification scheme to appropriately protect its IP. Data classification schemes allow an organization to prioritize controls around "crown jewels" IP that are essential to the viability of its business model, as compared to low value IP that requires less-stringent security protections.

Per the World Trade Organization (WTO), IP can be defined in several ways:

- Copyright and rights related to copyright (e.g., literary and artistic works); and
- Industrial property:
  - Trademarks;
  - Patents;
  - Industrial designs; and
  - Trade secrets.

Attorney-Client Privilege Information (ACPI)

ACPI is information between a client and his/her attorney, which may include other forms of sensitive information pertaining to the legal advice being sought (e.g., IP, CUI, FCI, PHI, PD, ITAR, etc.).

Per rule 1.6(c) of the American Bar Association's Model Rules of Professional Conduct, an attorney "*A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client*."

Per Cornell Law School's Legal Information Institute:

- Attorney-client privilege refers to "*a legal privilege that works to keep confidential communications between an attorney and his or her client secret. The privilege is asserted in the face of a legal demand for the communications, such as a discovery request or a demand that the lawyer testify under oath*."
- The work product doctrine refers to data protections, where "*an adverse party generally may not discover or compel disclosure of written or oral materials prepared by or for an attorney in the course of legal representation, especially in preparation for litigation*."

Student Educational Records

Per 34 CFR § 99.3, an "education record" is defined as records that are:

- Directly related to a student; and
- Maintained by an educational agency or institution or by a party acting for the agency or institution.

Export-Controlled Data

Per 15 CFR § 730-774, the U.S. Department of Commerce regulates the export of "dual-use" items according to the Export Administration Regulations (EAR). EAR items include goods and related technology, including technical data and technical assistance, which are designed for commercial purposes, but which could have military applications.

The list of EAR-controlled items, commonly referred to as the Commerce Control List (CCL).[23] The CCL categorizes these covered items into 10 broad categories:

1. Nuclear Materials, Facilities and Equipment, and Miscellaneous;
2. Materials, Chemicals, Microorganisms, and Toxins;

[23] *Commerce Control List - https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl*

3. Materials Processing;
4. Electronics;
5. Computers;
6. Telecommunications and Information Security;
7. Lasers and Sensors;
8. Navigation and Avionics;
9. Marine; and
10. Propulsion Systems, Space Vehicles, and Related Equipment.

EAR covers a broad range of categories:

- "Technical Data" may take forms such as:
  - Blueprints;
  - Plans;
  - Diagrams;
  - Models;
  - Formulae;
  - Tables;
  - Engineering designs and specifications; and
  - Manuals and instructions.
- "Technical Assistance" may take forms such as:
  - Instruction;
  - Skills training; and
  - Consulting services.

Within EAR, there are country-specific restrictions:

- D:1 (National Security);
- D:2 (Nuclear);
- D:3 (Chemical & Biological);
- D:4 (Missile Technology);
- D:5 (US Arms Embargoed Countries);
- E:1 (Terrorist Supporting Countries); and
- E:2 (Unilateral Embargo).

CRITICAL INFRASTRUCTURE INFORMATION (CII)

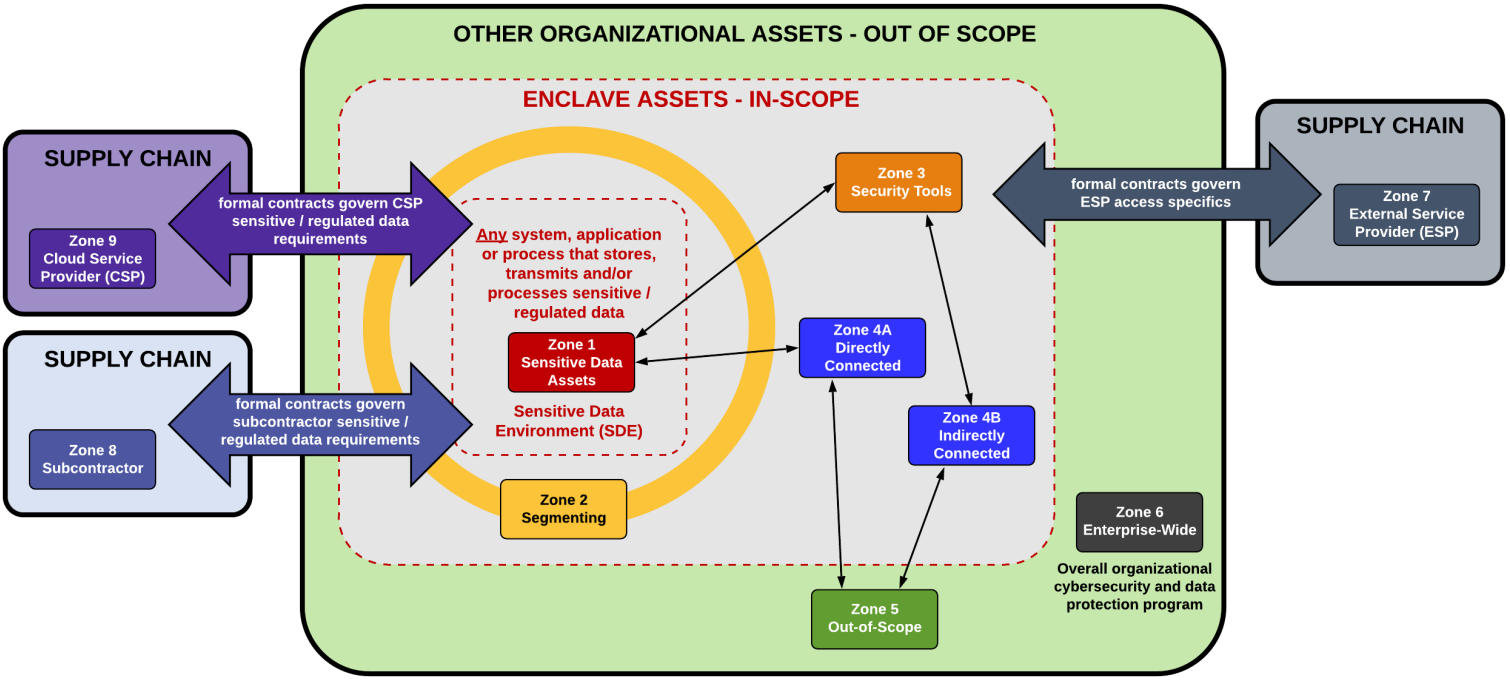
Per Section 671(3) of the Critical Infrastructure Information Act of 2002 (6 U.S.C. 131(3)), CII is defined as information not customarily in the public domain and related to the security of critical infrastructure or protected systems:

A. Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
B. The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
C. Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

ZONE-BASED APPROACH TO IMPLEMENTING DATA-CENTRIC SECURITY PROTECTIONS

When viewing scoping, there are nine (9) zones for sensitive/regulated data compliance purpose:

1. **Sensitive Data Assets (SDA)**: The first zone contains systems, services and applications that directly P/S/T sensitive/regulated data.
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, embedded technologies, applications or services that have some direct or indirect connection into the sensitive/regulated data environment. Systems, embedded technologies, applications and services that may impact the security of (for example, name resolution or web redirection servers) the sensitive/regulated data environment are always in scope. Essentially, it something can impact the security of sensitive/regulated data, it is in scope.
5. **Out-of-Scope**. The fifth zone contains out-of-scope systems that are completely isolated from the sensitive/regulated data systems.
6. **Enterprise-Wide**. The sixth zone addresses the organization's overall corporate security program (cyber and physical).
7. **External Service Provider (ESP)**. The seventh zone addresses supply-chain security with the "flow down" of contractual requirements to ESPs that can directly or indirectly influence the sensitive/regulated data environment. ESPs are independent, third-party organization that provides services, including but not limited to:
    a. Consulting/professional services;
    b. Software development;
    c. Staff augmentation; and
    d. Technology support (e.g., Managed Services Provider (MSP)).
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 (sensitive/regulated data).
9. **Cloud Service Providers (CSP).** The ninth zone addresses CSPs, which are a specialized form of ESP. An ESP is a CSP when it offers "cloud computing services" that enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five (5) essential characteristics, three (3) service models and four (4) deployment models:
    a. Essential Characteristics:
        1. On-demand self-service;
        2. Broad network access;
        3. Resource pooling;
        4. Rapid elasticity; and
        5. Measured service.
    b. Service Models:
        1. Software as a Service (SaaS);
        2. Platform as a Service (PaaS); and
        3. Infrastructure as a Service (IaaS).
    c. Deployment Models:
        1. Private cloud;
        2. Community cloud;
        3. Public cloud; and
        4. Hybrid cloud.



ZONE 1: SENSITIVE DATA ASSETS

Zone 1
Sensitive Data Assets

All systems, applications and services that P/S/T sensitive/regulated data are Category 1 devices. These systems that interact with sensitive/regulated data are the main assets that sensitive/regulated data are trying to protect.

ZONE 2: SEGMENTING

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 "sensitive/regulated data contamination" from the sensitive/regulated data environment to uncontrolled environments. Typically, these are firewalls or segmentation technology that implement some form of Access Control List (ACL) to restrict logical access into and out of the sensitive/regulated data environment. This can also include Zero Trust Architecture (ZTA) components that provide micro-segmentation services.

Note: If network segmentation is in place and is being used to reduce the scope of an 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.

ZONE 3: SECURITY TOOLS

Zone 3
Security Tools

All systems that provide security-related services or IT-enabling services that may affect the security of the sensitive/regulated data 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; and
- Intrusion Detection Systems/ Intrusion Prevention Systems (IDS/IPS).

ZONE 4: CONNECTED

Zone 4 Connected

Any system that has some capability to communicate with systems, applications or services within the sensitive/regulated data environment is a Category 4 device. A "connected" system, embedded technologies, application or service should be considered in scope for since it is not completely isolated. If it can potentially impact the security of sensitive/regulated data, it is in scope.

There are two sub-categories of connected devices:

- Directly Connected; and
- Indirectly Connected.

ZONE 4A: DIRECTLY CONNECTED

Zone 4A Directly Connected

This sub-category addresses any system that is "connected to" the sensitive/regulated data environment is considered a directly-connected system. Any system outside of the sensitive/regulated data environment that is capable of communicating with a system that P/S/T sensitive/regulated data (e.g., asset within the sensitive/regulated data environment) is a Category 4A device.

Note: For systems outside of the sensitive/regulated data environment that have periodic controlled and managed outbound connections from the sensitive/regulated data environment that do not involve the transfer of regulated data (sensitive/regulated data), 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 sensitive/regulated data. 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 4B: INDIRECTLY CONNECTED

Zone 4B Indirectly Connected

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

ZONE 5: OUT-OF-SCOPE

Zone 5 Out-of-Scope

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

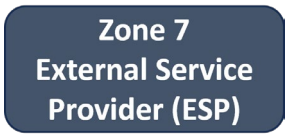
Four (4) tests must be considered to confirm that a system is out-of-scope and considered a Category 5 asset. This amounts to ensuring that the asset does not fall under the previously defined categories:

1. System components do not P/S/T sensitive/regulated data.
2. System components are not on the same network segment or in the same subnet or VLAN as systems, applications or processes that P/S/T sensitive/regulated data.
3. System components cannot connect to or access any system in the sensitive/regulated data environment.
4. System components cannot gain access to the sensitive/regulated data environment, nor impact a security control for a system, embedded technologies, application or service in the sensitive/regulated data environment via an in-scope system.

ZONE 6: ENTERPRISE WIDE

This category addresses enterprise-wide security controls that exist outside of just the sensitive/regulated data environment. 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: EXTERNAL SERVICE PROVIDER (ESP)



Sensitive/regulated data in the supply chain needs to be taken seriously and this category addresses External Service Providers (ESPs). The formal contracts between your organization its ESPs dictate the logical and physical access those ESP have to the organization's facilities, systems and data. The "flow down" considerations of sensitive/regulated data must be addressed with each ESP to clearly identify the ESPs' ability to directly or indirectly influence the sensitive/regulated data environment.

Examples of ESPs that may have sensitive/regulated data flow down requirements:

- Bookkeeping services;
- Human Resource (HR) recruiters;
- Payroll providers;
- Educational training providers (e.g., Computer Based Training (CBT));
- IT service providers/cybersecurity consultants/Managed Service Provider (MSP)/Managed Security Services Provider (MSSP);
- Business process consultants;
- Project Managers (PMs);
- Document destruction providers; and
- Janitorial services and environmental control management.

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 sensitive/regulated data.

ZONE 9: CLOUD SERVICE PROVIDERS (CSP)

This category addresses ESP providing cloud computing services that enable ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A CSP can be identified by its function, since the cloud model is composed of five (5) essential characteristics, three (3) service models and four (4) deployment models: [24]

Essential Characteristics:

1. On-demand self-service;
2. Broad network access;
3. Resource pooling;
4. Rapid elasticity; and
5. Measured service.

Service Models:

1. Software as a Service (SaaS);
2. Platform as a Service (PaaS); and
3. Infrastructure as a Service (IaaS).

Deployment Models:

1. Private cloud;
2. Community cloud;
3. Public cloud; and
4. Hybrid cloud.

Examples of CSPs that may have sensitive/regulated data flow down requirements:

- Cloud hosting environments, including but not limited to:
  - Amazon Web Services (AWS);
  - Microsoft Azure;
  - Google Cloud;
  - Oracle Cloud; and
  - IBM Cloud.
- Hosted applications, including but not limited to:
  - Vulnerability scanners;
  - Remote Monitoring & Management (RMM) solutions;
  - Patch management solutions;
  - Endpoint Detection and Response (EDR) solutions
  - Educational training providers/CBT;
  - File sharing;
  - E-mail;
  - Video teleconferencing;
  - Bookkeeping software (e.g., QuickBooks Online);
  - Personnel management software; and
  - Payroll services.

[24] *32 CFR Part 170 & NIST SP 800-145 - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*

IN-SCOPE MATRIX

The following chart summarizes the concept of what may or may not be in scope:

Zone	Segmentation Method	Is Sensitive/Regulated Data P/S/T?	In Scope?
Zone 1 Sensitive Data 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 ESPs	Must Be Determined	**MAYBE**	**MAYBE**
Zone 8 Subcontractors	Must Be Determined	**MAYBE**	**MAYBE**
Zone 9 CSPs	Controlled Access	**MAYBE**	**MAYBE**

System-to-System Communications

The following chart summarizes the concept of what communications should or should not be in-scope for sensitive/regulated data:

Sensitive Data Communications Matrix	Zone 1 Sensitive Data Assets	Zone 2 Segmenting	Zone 3 Security Tools	Zone 4 Connected	Zone 5 Out-of-Scope	Zone 6 Enterprise Wide	Zone 7 ESPs	Zone 8 Subcontractors	Zone 9 CSPs
Zone 1 Sensitive Data Assets	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**NO** *Isolated*	**NO** *Isolated*	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**
Zone 2 Segmenting	**IN-SCOPE**	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**NO** *Isolated*	**NO** *Isolated*	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**
Zone 3 Security Tools	**IN-SCOPE**	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**NO** *Isolated*	**NO** *Isolated*	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**
Zone 4 Connected	**IN-SCOPE**	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**NO** *Isolated*	**NO** *Isolated*	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**
Zone 5 Out-of-Scope	**NO** *Isolated*	**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*	**NO** *Isolated*
Zone 7 ESPs	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**NO** *Isolated*	**NO** *Isolated*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*
Zone 8 Subcontractors	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**NO** *Isolated*	**NO** *Isolated*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*
Zone 9 CSPs	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**IN-SCOPE**	**NO** *Isolated*	**NO** *Isolated*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*	**Possibly** *Controlled Access*

Note: For systems, applications and services (asset) outside of the SDE that have periodic outbound connections from the sensitive/regulated data environment that do not involve the transfer of sensitive/regulated data, there is a case to argue that the asset could be ruled out-of-scope since it does not have a direct impact on the security of sensitive/regulated data.

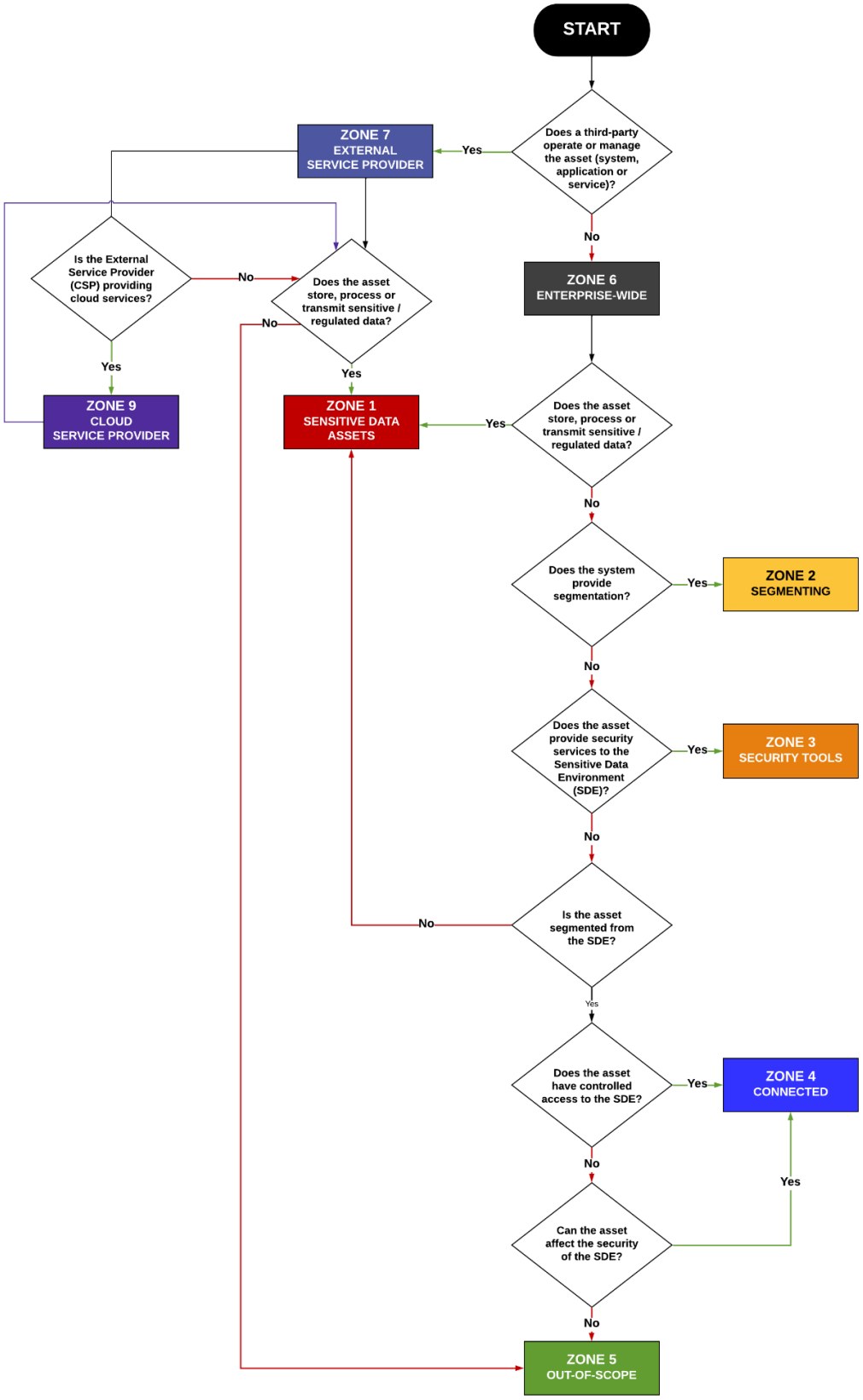
EXAMPLES - ASSET CATEGORIZATIONS

The following examples are for reference purposes only and should not be viewed as authoritative guidance, since it is your obligation to perform appropriate due diligence based on your specific operating parameters:

USG Zone	Technology Tools Categories
Zone 1 Sensitive Data Asset (SDA)	Backup Tools (BCDR)
	Data Destruction Tools
	Data Storage (e.g., file servers, databases, etc.)
	Virtual Desktop Infrastructure (VDI) - Server
Zone 2 Segmenting	Access Control List (ACL) Tools
	Network Firewall
	Zero Trust (ZT) Tools
Zone 3 Security Tools	Antimalware / Antispam
	Application Security Testing
	Centralized Log Management / SIEM / Event Log Monitoring
	Certificate Management Tools / Public Key Infrastructure (PKI)
	Change Control Tools
	Configuration Management Database (CMDB)
	Content / DNS Filtering Tools
	Cryptographic Tools (data at rest)
	Data Loss Prevention (DLP)
	Endpoint Detection and Response (EDR)
	File Integrity Monitoring (FIM)
	Forensics Tools
	Governance, Risk & Compliance (GRC)
	Identity & Access Management (IAM)
	Intrusion Detection / Prevention System (IDS / IPS)
	Mobile Device Management (MDM)
	Multi-Factor Authentication (MFA)
	Network Baseline Management Tools
	Patch Management Tools
	Penetration Testing Tools
	Privileged Access Management (PAM)
	Sandbox / Detonation Chamber Tools
	Secure Baseline Configurations (SBC) Tools
	Secure File Sharing
	Security Orchestration, Automation and Response (SOAR)
	Threat Intelligence Tools
	Vulnerability Scanning Tools
	Wireless Intrusion Prevention /Detection System (WIPS/WIDS)
	Email Tools
	IT Asset Management (ITAM)
	Learning Management System (LMS)
	Physical Access Control (PAC) Tools
	Remote Access Tools / VPN Concentrator
	Risk Register / POA&M Tools
	VDI Endpoint
	Voice over Internet Protocol (VoIP)
Zone 6	Visitor Management

ASSET SCOPING DECISION TREE

The following decision tree provides a logical walk-through to determine if an asset is in scope or not:[25]



[25] https://complianceforge.com/content/pdf/unified-scoping-guide-decision-tree-diagram.pdf

ZERO TRUST ARCHITECTURE (ZTA) SCOPING GUIDANCE

The path forward for the US Government is towards Zero Trust (ZT). Therefore, it is important to address how ZT integrates with this scoping guide.

ZERO TRUST PRACTICES

There are several industry-recognized leaders in determining Zero Trust Architecture (ZTA):

- NIST 800-207 - Zero Trust Architecture;
- NIST National Cybersecurity Center of Excellence (NNCoE);
- US Department of Defense; and
- DHS CISA.

NIST SP 800-207 – ZERO TRUST ARCHITECTURE

NIST SP 800-207 *Zero Trust Architecture*, is a worthwhile introduction into ZTA, since it addresses high-level concepts, where it covers logical components, possible deployment scenarios and threat considerations. [26] NIST SP 800-207 also presents a general road map for organizations wishing to migrate to ZTA. NIST makes it clear that ZT is not a single architecture but a set of guiding principles for workflow, system design and operations that can be used to improve the security posture of any classification or sensitivity level.

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (NNCOE)

As of the date of this document, the NNCoE is on its Initial Public Draft (IPD) version of NIST SP 1800-35, *Implementing a Zero Trust Architecture*. [27] This guidance from NIST contains "enterprise build guidance" for common technologies (e.g., implementing ZTA in Microsoft Azure with Entra Conditional Access and Intune).

NIST SP 1800-25 provides a starting point for an organization's IT and security architects to craft a ZTA strategy for their specific operational criteria based on seven (7) tenets of ZT:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated asset.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

DOD ZERO TRUST OVERLAYS

The DoD's Zero Trust Strategy is US military-focused, so it has limited applicability outside the military industrial complex. However, the DoD's guiding principles provides useful guardrails when making decisions regarding how best to implement the ZTA. [28]

The DoD defined five (5) major ZT tenets in the DoD Zero Trust Reference Architecture, Version 2.0. These DoD tenets represent foundational elements and influence all aspects of DoD's zero trust implementation.3

1. Assume a hostile environment.
2. Presume breach.
3. Never trust, always verify.
4. Scrutinize explicitly.
5. Apply unified analytics.

---

[26] *NIST SP 800-27 - https://csrc.nist.gov/pubs/sp/800/207/final*
[27] *NIST SP 1800-35 - https://csrc.nist.gov/pubs/sp/1800/35/ipd*
[28] *DoD Zero Trust Overlays - https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf*

DHS CISA Zero Trust Capability Framework (ZTCF)

The Department of Homeland Security (DHS) created a draft framework based on ZT capability, for the following three (3) reasons:

1. Existing ZTA across the US Federal government focus on the attack surface but lack definition of, or focus on, protect surfaces.
2. Assessment of ZT capability using existing ZTA has proven difficult, because most architectures focus on defining ZT, not on assessing ZT capability.
3. Prioritization of ZT investments using existing ZTA is also difficult, because current architectures are not designed to prioritize organizational effort or investment.

Organizations can refer to the DHS Zero Trust Implementation Strategy for general background on ZT.[29]

Zero Trust Technology Categorizations

ZT technologies will be categorized as:

- Zone 2 – Segmenting; and
- Zone 3 – Security Tools.

The justification for the placement in these zones is the primary function of ZT controls.

[29] *DHS ZT Implementation Strategy - https://www.dhs.gov/publication/zero-trust-implementation-strategy*

CMMC – Department of Defense Scoping Guidance

32 CFR Part 170 does not change the five (5) existing categories of assets per CMMC scoping guidance from the US DoD Chief Information Officer (CIO):[30]

1. CUI Assets;
2. Security Protection Assets (SPA);
3. Contractor Risk Managed Assets (CRMA);
4. Specialized Assets (SA); and
5. Out-of-Scope Assets (OOSA).

32 CFR Part 170 Scoping Criteria

This also includes guidance from 32 CFR Part 170 on scoping criteria.

CMMC Level 1 Scoping Criteria

As specified in § 170.19(b) for CMMC Level 1 scoping:[31]

- All assets that P/S/T FCI are in scope; and
- All other assets are out-of-scope and are not considered in the CMMC Level 1 assessment.

CMMC Level 2 Scoping Criteria

As specified in § 170.19(c) for CMMC Level 2 scoping: [32]

- All assets that P/S/T CUI are in scope; and
- All assets that provide security protections for these assets are in scope, but:
  - Contractor Risk Managed Assets (CRMA):
    - Must be documented; and
    - Are subject to a limited check.
  - Specialized Assets (SA):
    - Must be documented; but
    - Are not assessed against other CMMC security requirements.
- All other assets are out-of-scope and are not considered in the CMMC Level 2 assessment.

CMMC Level 3 Scoping Criteria

As specified in § 170.19(d) for CMMC Level 3 scoping: [33]

- All assets that can (whether intended to or not) or do P/S/T CUI are in scope;
- All assets that provide security protections for these assets are in scope:
  - This includes Specialized Assets (SA), but allows an intermediary device to provide the capability for the SA to meet one or more CMMC security requirements, as needed; and
  - These assets (or the applicable intermediary device, in the case of SA) are fully assessed against the applicable CMMC security requirements; and
- All other assets are out-of-scope and are not considered in the CMMC Level 3 assessment.

External Service Provider (ESP) & Cloud Service Provider (CSP) Scoping Criteria

When utilizing an ESP that is a CSP: [34]

- For CUI (with or without) Security Protected Data (SPD):
  - The CSP shall meet the FedRAMP requirements in 48 CFR 252.204–7012.
- SPD (without CUI)
  - The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets (SPAs).
- Neither CUI nor SPD:

---

[30] *DoD CIO CMMC Resources & Documentation - https://dodcio.defense.gov/CMMC/Resources-Documentation/*
[31] *32 CFR Part 170.19 - https://www.federalregister.gov/d/2024-22905/p-181*
[32] *32 CFR Part 170.19 - https://www.federalregister.gov/d/2024-22905/p-182*
[33] *32 CFR Part 170.19 - https://www.federalregister.gov/d/2024-22905/p-183*
[34] *32 CFR Part 170.19(c)(2)(i) - https://www.federalregister.gov/d/2024-22905/p-2335*

- None - a service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

When utilizing an ESP that is not a CSP: [35]

- For CUI (with or without) Security Protected Data (SPD):
  - The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
- SPD (without CUI)
  - The services provided by the ESP are in the OSA's assessment scope and shall be assessed as SPAs.
- Neither CUI nor SPD:
  - None - a service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP

Per the DoD CIO's CMMC Level 2 Scoping Guide, an ESP: [36]

- Can be within the OSA's scope of CMMC requirements if it meets CUI Asset and/or SPA criteria. To be considered an ESP, data (specifically CUI or SPA) must reside on the ESP assets.
- May utilize cloud offerings to deliver services to clients without being a CSP.
- Managing a third-party cloud service on behalf of an OSA would not be considered a CSP.
- Providing technical support services to its clients would be considered a Managed Service Provider (MSP), since it does not host its own cloud platform offering.
- Would be considered a CSP when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Categories of CMMC Assets

The following categories of assets are per CMMC scoping guidance from the US DoD CIO to provide context for how the DoD views these as in-scope vs out-of-scope: [37]

CUI Asset

A CUI Asset has different definitions, based on the CMMC Level: [38]

- For CMMC Level 2:
  - An asset that P/S/T CUI.
- For CMMC Level 3:
  - Assets that P/S/T CUI; and
  - Assets that can, but are not intended to P/S/T CUI.

CMMC Level 2 Organizations Seeking Assessment (OSA) Requirements – CUI Asset:

1. Document in the asset inventory;
2. Document asset treatment in the System Security Plan (SSP);
3. Document in the network diagram of the CMMC Assessment Scope; and
4. Prepare to be assessed against CMMC Level 2 security requirements.

CMMC Level 2 Assessment Requirements – CUI Asset:

1. Assess against all Level 2 security requirements.

CMMC Level 3 Organizations Seeking Certification (OSC) Requirements – CUI Asset:

1. Document in the asset inventory;
2. Document asset treatment in the System Security Plan (SSP);
3. Document in the network diagram of the CMMC Assessment Scope; and

---

[35] *32 CFR Part 170.19(c)(2)(i) - https://www.federalregister.gov/d/2024-22905/p-2335*
[36] *DoD CIO ESP Considerations- https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=12*
[37] *DoD CIO CMMC Resources & Documentation - https://dodcio.defense.gov/CMMC/Resources-Documentation/*
[38] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=5*

4. Prepare to be assessed against CMMC Level 2 security requirements.

CMMC Level 3 Assessment Requirements – CUI Asset:

1. Assess against all Level 2 security requirements.

Security Protection Asset (SPA)

Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope, irrespective of whether or not these assets P/S/T CUI. For example, an ESP that provides a Security Information and Event Management (SIEM) service may be separated logically and may not process CUI, but the SIEM does contribute to meeting the CMMC requirements within the OSA's CMMC Assessment Scope.

SPAs are: [39]

- In-scope for CMMC; and
- Required to conform to applicable CMMC controls, regardless of their physical or logical placement.

SPAs cover people, technologies and facilities, as shown below: [40]

Asset Type	SPA Examples
People	▪ Consultants who provide cybersecurity service ▪ Managed service provider personnel who perform system maintenance ▪ Enterprise network administrators
Technology	▪ Cloud-based security solutions ▪ Hosted Virtual Private Network (VPN) services ▪ SIEM solutions
Facility	▪ Co-located data centers ▪ Security Operations Centers (SOCs) ▪ OSA office buildings

CMMC Level 2 OSA Requirements – SPA:

1. Document in the asset inventory;
2. Document asset treatment in SSP;
3. Document in the network diagram of the CMMC Assessment Scope; and
4. Prepare to be assessed against CMMC Level 2 security requirements.

CMMC Level 2 Assessment Requirements – SPA:

1. Assess against Level 2 security requirements that are relevant to the capabilities provided.

CMMC Level 3 OSC Requirements – SPA:

1. Document in the asset inventory;
2. Document asset treatment in SSP;
3. Document in the network diagram of the CMMC Assessment Scope; and
4. Prepare to be assessed against CMMC Level 2 security requirements.

CMMC Level 3 Assessment Requirements – SPA:

2. Assess against Level 2 security requirements that are relevant to the capabilities provided.

Contractor Risk Managed Asset (CRMA)

CRMA are assets that: [41]

- Can, but are not intended to, P/S/T CUI because of security policy, procedures, and practices in place; and
- Are not required to be physically or logically separated from CUI assets.

CRMA are:

---

[39] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=5*
[40] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=8*
[41] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=5*

- In-scope for CMMC;
- Not required to be physically or logically separated from CUI Assets;
- Managed according to the contractor's enterprise-wide cybersecurity policies, standards, procedures and practices; and
- Not assessed against CMMC-specific controls.

There is conflicting guidance in the DoD CIO's CMMC Level 2 Scoping Guide for CRMA and the lack of clarity creates ambiguity in defining actual baseline requirements: [42]

- CRMA are described as assets that:
  - Can, but are not intended to P/S/T CUI because of security policy, procedures and practices in place; and
  - Are not required to be physically, or logically, separated from CUI Assets.
- OSA's requirements for CRMA include:
  - The CRMA must be documented in:
    - Asset inventory;
    - System Security Plan (SSP) (e.g., describe how CRMA are protected); and
    - Network diagrams; and
  - The OSA must prepare to be assessed against CMMC Level 2 security requirements.
- CRMA assessment requirements focus on the assessor reviewing the SSP for details about CRMA:
  - If "sufficiently documented," the assessor is not to assess CRMA against other CMMC security requirements; and
  - If the OSA's organization-wide policies, standards and procedures, or other findings, raise questions about CRMA assets, the assessor can conduct a limited check to identify deficiencies with CRMA. These "limited checks":
    - Shall not materially increase the assessment duration nor the assessment cost; and
    - Will be assessed against CMMC security requirements.

The issues with this ambiguity are:

- The use of the term for CRMA to be assessed using "risk-based security policies, procedures, and practices" is shared with Specialized Assets (SA). While SA are in-scope, SA are not assessed against CMMC security requirements.
- There are no definitions for the following terms, which opens the OSA up to assessment creep from a rogue assessor:
  - Sufficiently documented – who decides what is sufficient?
  - Materially – who determines the financial or operational impact to be considered material for an assessment?
  - Limited checks – what constitutes the level of rigor associated with this term?
- While the OSA can leverage its non-CMMC policies, standards and procedures for CRMA, it is at the whim of the assessor to determine what is acceptable. **This ambiguity means OSA should plan to protect CRMA according to NIST 800-171 / NIST 800-171A requirements.**

CMMC Level 2 OSA Requirements – CRMA:

1. Document in the asset inventory;
2. Document asset treatment in the SSP;
3. Document in the network diagram of the CMMC Assessment Scope; and
4. Prepare to be assessed against CMMC Level 2 security requirements.

CMMC Level 2 Assessment Requirements – CRMA:

1. Review the SSP:
   a. If sufficiently documented, do not assess against other CMMC security requirements, except as noted;
   b. If OSA's risk-based security policies, procedures, and practices documentation or other findings raise questions about these assets, the assessor can conduct a limited check to identify deficiencies;
   c. The limited check(s) shall not materially increase the assessment duration nor the assessment cost; and
   d. The limited check(s) will be assessed against CMMC security requirements.

[42] *DoD CIO ESP Considerations- https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=12*

SPECIALIZED ASSET (SA)

SA are assets that can P/S/T CUI but are unable to be fully secured, including: [43]

- Internet of Things (IoT) devices;
- Industrial Internet of Things (IIoT) devices;
- Operational Technology (OT);
- Government Furnished Equipment (GFE);
- Restricted Information Systems (RIS); and
- Test Equipment.

For additional clarity: [44]

- Government Furnished Equipment (GFE) is all equipment owned or leased by the government and includes OSA-acquired equipment that is based on government required specifications and/or configurations. Government Furnished Equipment does not include intellectual property or software [Reference: Federal Acquisition Regulation (FAR) 52.245-1].
- Internet of Things (IoT) or Industrial Internet of Things (IIoT) means the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, as defined in NIST SP 800-172A. They are interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include:
  - Smart electric grids;
  - Lighting;
  - Heating;
  - Air conditioning, and
  - Fire and smoke detectors.
- Operational Technology (OT) means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. OT includes, but is not limited to:
  - Industrial control systems (ICS);
  - Building management systems;
  - Fire control systems
  - Physical access control mechanisms;
  - Supervisory Control and Data Acquisition (SCADA) systems;
  - Programmable Logic Controllers (PLCs);
  - Computerized Numerical Control (CNC) devices;
  - Machine controllers;
  - Fabricators;
  - Assemblers; and
  - Machining technologies.
- Restricted Information Systems (RIS) means systems [and associated Information Technology (IT) components comprising the system] that are configured based on government security requirements (i.e., connected to something that was required to support a functional requirement) and are used to support a contract (e.g., fielded systems, obsolete systems, and product deliverable replicas).
- Test Equipment means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. It can include hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

Specialized Assets are part of the CMMC Assessment Scope. OSAs are required to document these assets in a SSP and detail how SAs are managed using the OSA's: [45]

- Risk-based information security policy;
- Procedures; and

---

[43] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=5*
[44] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=9*
[45] *32 CFR Part 170.19(c)(2)(1) - https://www.federalregister.gov/d/2024-22905/p-2334*

- Practices.

CMMC Level 2 OSA Requirements – SA:

1. Document in the asset inventory;
2. Document asset treatment in the SSP;
3. Show these assets are managed using the contractor's risk-based security policies, procedures, and practices; and
4. Document in the network diagram of the CMMC Assessment Scope.

CMMC Level 2 Assessment Requirements – SA:

1. Review the SSP; and
2. Do not assess against other CMMC security requirements.

CMMC Level 3 OSC Requirements – SA:

1. Document in the asset inventory;
2. Document asset treatment in the SSP;
3. Show these assets are managed using the contractor's risk-based security policies, procedures, and practices; and
4. Document in the network diagram of the CMMC Assessment Scope.

CMMC Level 3 Assessment Requirements – SA:

1. Review the SSP; and
2. Do not assess against other CMMC security requirements.

Out of Scope Asset (OOSA)

OOSA are: [46]

- Assets that:
  - Cannot P/S/T CUI; and do not provide security protections for CUI Assets;
  - Are physically or logically separated from CUI assets; and
  - Fall into any in-scope asset category cannot be considered an OOSA; and
- An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset.

CMMC Level 2 OSA Requirements – OOSA:

1. Prepare to justify the inability of an OOSA to P/S/T CUI.

CMMC Level 2 Assessment Requirements – OOSA:

1. None.

[46] *DoD CIO CMMC Asset Categories - https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf#page=5*

UNIFIED SCOPING GUIDE (USG) ZONES VS CMMC SCOPING GUIDE ASSET CATEGORIZATIONS

The chart below shows how CMMC 2.0 Level 2 scoping guidance complements the USG's zone model. The table should be viewed as a generic example, since it may not be applicable to every organization's infrastructure and should only be viewed as an educational guide to compare the USG vs CMMC scoping terms:

CUI Scoping Guide Applicability Matrix	CUI Asset	Security Protection Asset (SPA)	Contractor Risk Managed Asset (CRMA)	Specialized Asset (SA)	Out of Scope Asset (OOSA)
Zone 1 Sensitive Data Assets	CUI Asset	N/A	N/A	SA	N/A
Zone 2 Segmenting	N/A	SPA	N/A	N/A	N/A
Zone 3 Security Tools	N/A	SPA	N/A	N/A	N/A
Zone 4 Connected	N/A	N/A	CRMA	SA	N/A
Zone 5 Out-of-Scope	N/A	N/A	N/A	SA	OOSA
Zone 6 Enterprise Wide	N/A	N/A	N/A	SA	OOSA
Zone 7 ESPs	Possibly CUI Asset	Possibly SPA	N/A	Possibly SA	Possibly OOSA
Zone 8 Subcontractors	Possibly CUI Asset	Possibly SPA	N/A	Possibly SA	Possibly OOSA
Zone 9 CSPs	Possibly CUI Asset	Possibly SPA	N/A	Possibly SA	Possibly OOSA

For a generic CMMC Level 2 scoping exercise, within the USG's model:

- **CUI Assets** would be considered **Sensitive Data Assets (Zone 1).**
- Based on the asset, **Security Protection Assets (SPA)** would be considered either:
  - **Segmenting (Zone 2)**; or
  - **Security Tools (Zone 3)**.
- **Contractor Risk Managed Assets (CRMA)** would be considered **Connected (Zone 4)** since they are capable or P/S/T CUI but do not due to the OSA's policies, standards and/or procedures.
- **Specialized Assets (SA)** would be considered either:
  - **Sensitive Data Assets (Zone 1)**;
  - **Connected (Zone 4)**;
  - **Out-of-Scope (Zone 5)**;
  - **ESPs (Zone 7)**;
  - **Subcontractors (Zone 8)**; and/or
  - **CSPs (Zone 9)**.
- **Out-of-Scope Assets (OOSA)** would be considered **Out-of-Scope (Zone 5)** that could exist in:
  - **Enterprise Wide (Zone 6)**;
  - **ESPs (Zone 7)**;
  - **Subcontractors (Zone 8)**; and/or
  - **CSPs (Zone 9)**.

EXAMPLE NETWORK SCOPING SCENARIOS

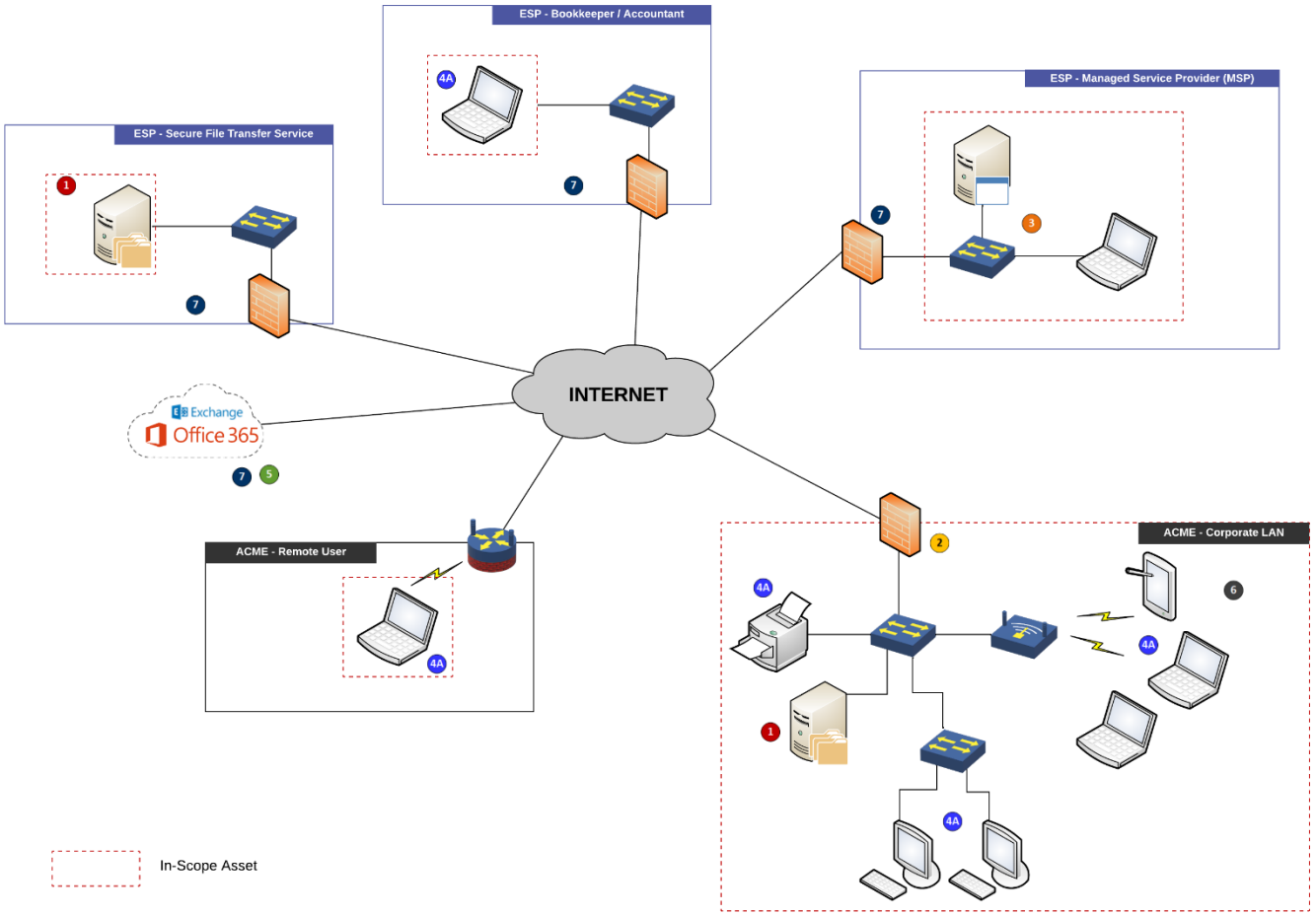
These scenarios are for reference purposes only to help you visualize walking through your data flows and network diagrams to identify what assets are in-scope and what is out-of-scope.

SCENARIO 1: CUI ON A FLAT NETWORK

In this scenario, ACME Consulting (ACME) is the Organization Seeking Assessment (OSA) and is a subcontractor on a project to manufacture an antenna for a DoD weapons system. The dimensions of the antenna are categorized as Controlled Unclassified Information (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 CMMC Level 2 organization, since it P/S/T 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 External Service Providers (ESP) 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 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 2 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.

Organizations – Corporate LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**). **CMMC – OOSA**
- ACME has a single firewall that connects to the Internet Service Provider (ISP) (**zone 2**). **CMMC – SPA**
- ACME utilizes a Network Attached Storage (NAS) device to store CUI (**zone 1**). **CMMC – CUI Asset**
- Several organizations users have CUI on their workstations (**zone 1**) **CMMC – CUI Asset**. However, the majority of the organization's users do not have CUI their workstations, but due to a lack of segmentation, all corporate assets are in-scope (**zone 4a**). **CMMC – CRMA**
- Email (Office 365) is administratively out of scope due to business practices prohibiting CUI from being emailed (**zones 5 & 7**). **CMMC – CRMA**

Organizations – 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. **CMMC – CUI Asset**

Managed Service Provider (MSP)

- IT technicians from the MSP use Remote Monitoring & (RMM) tools to manage the ACME corporate LAN (**zones 3 & 7**) **CMMC – SPA**.
- ACME has a written contract with the MSP that documents its security-related roles and responsibilities for the MSP (**zone 7**). **CMMC – SPA**
- IT technicians use RMM to connect to ACME assets that have access to systems that P/S/T CUI (**zones 4a & 7**) and fall within scope for the Level 2 assessment. **CMMC – SPA**
- Other "security tools" the MSP uses protect ACME's corporate LAN have direct access to devices that P/S/T CUI (**zones 3 & 7**) **CMMC – SPA**. 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. Bookkeeper/accountant would be an External Service Provider (ESP) and their assets would be CRMA, since they could technically S/P/T CUI through the VPN, they are administratively prohibited (**zones 4a & 7**). **CMMC – CRMA**
- ACME has a written contract with the bookkeeper/accountant (**zone 7**). However, the bookkeeper/accountant assets directly connect to ACME assets that have access to systems that P/S/T CUI (**zone 4a**) and fall within scope for the Level 2 assessment. **CMMC – SPA**

Secure File Transfer Service

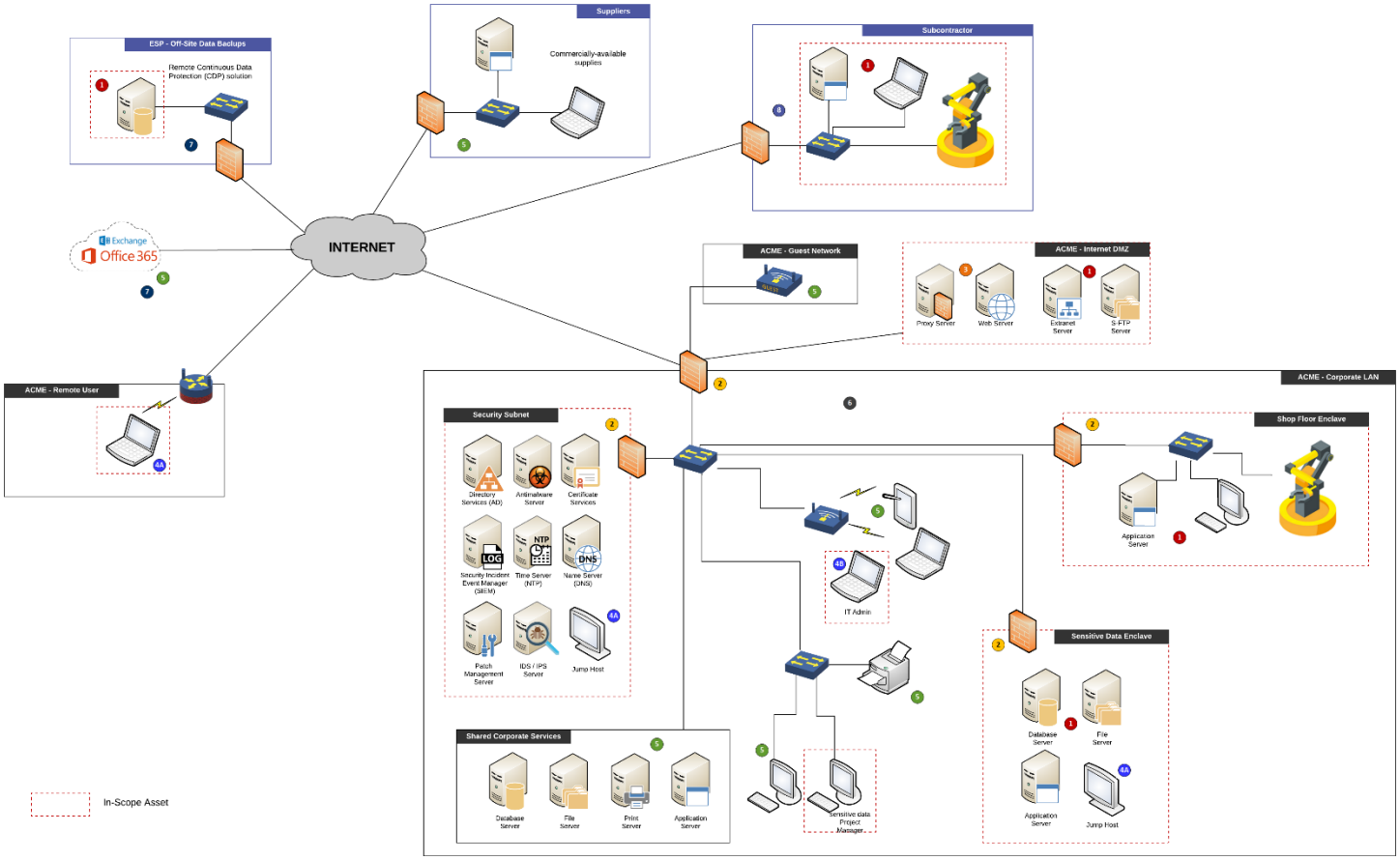
- Due to CUI being temporarily stored and transmitted in the file transfer service's systems, that takes that service within scope (**zones 1 & 7**) **CMMC – CUI Asset**. While sensitive/regulated data is encrypted in transit, applicable controls need to be reviewed and applied for instances where CUI may be at rest and accessible by MSP personnel.
- ACME has a written contract with the MSP that documents its security requirements (**zone 7**). **CMMC – SPA**
- The ESP 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 organizations must secure the secure file transfer service by implementing applicable controls associated with access control to appropriately protect the data being housed offsite.

SCENARIO 2: CUI ON A SEGMENTED NETWORK (ON-PREMISE INFRASTRUCTURE)

In this scenario, ACME Engineering (ACME) is the Organization Seeking Assessment (OSA) and is a subcontractor on a project to develop components for a DoD weapons system. The components are categorized as Controlled Unclassified Information (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 CMMC Level 2 organization, since it P/S/T 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 2 assessment.

ORGANIZATIONS – CORPORATE LAN

- **Corporate LAN**
  - Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**). CMMC – OOSA
  - The majority of the organization's corporate LAN (wired & wireless) are out-of-scope (**zone 5**) due to segmentation. CMMC – OOSA
  - 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**). CMMC – CRMA
  - Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zones 5 & 7**). CMMC – OOSA
- **CUI Enclave**
  - The firewall that provides segmentation services to sensitive/regulated data enclave is in scope (**zone 2**). CMMC – SPA
  - The database, file and application server all P/S/T CUI (**zone 1**). CMMC – CUI Asset
  - The jump host directly connects to zone 1 assets, so it is in scope (**zone 4a**). CMMC – SPA
- **Shop Floor Enclave**
  - The firewall that provides segmentation services to the shop floor enclave is in scope (**zone 2**). CMMC – SPA
  - The application server P/S/T CUI (**zone 1**). CMMC – OOSA
  - The manufacturing workstation and CNC machines P/S/T CUI (**zone 1**). CMMC – OOSA & CMMC – SA
- **Security Subnet**
  - The firewall that provides segmentation services to the security subnet is in scope (**zone 2**). CMMC – SPA
  - The jump host directly connects to zone 3 assets, so it is in scope (**zone 4a**). CMMC – CRMA
  - The "security tools" that protect both the corporate LAN and enclave is in scope (**zone 3**) CMMC – SPA. 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**). CMMC – OOSA

ORGANIZATIONS – INTERNET DMZ & GUEST NETWORK

- The Internet DMZ is in scope since it contains an extranet server that is used to P/S/T CUI (**zone 1**) CMMC – CUI Asset and the proxy server is in-scope (**zone 3**) CMMC – SPA since it provides security services.
- The "guest network" is segmented from the corporate LAN and is out-of-scope (**zone 5**). CMMC – OOSA

ORGANIZATIONS – REMOTE USER

- The remote users are not in scope (**zone 5**), since they do not have access to CUI. CMMC – OOSA
- 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.

EXTERNAL SERVICE PROVIDER (ESP) - SECURE FILE TRANSFER SERVICE

- Due to CUI being stored in the off-site backups, that takes that service within scope (**zones 1 & 7**). CMMC – CUI Asset
- ESP has a written contract with ACME that documents its security requirements (**zone 7**). CMMC – SPA
- The ESP is excluded from additional controls, since it has no access to the private key that encrypts the backed up data.
- The organizations must secure the secure file transfer service by implementing 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 (**zones 1 & 8**). **CMMC – CUI Asset**

- ACME has a written contract with its subcontractors that documents the security requirements to protect CUI (**zone 8**). **CMMC – CUI Asset**

SUPPLIERS

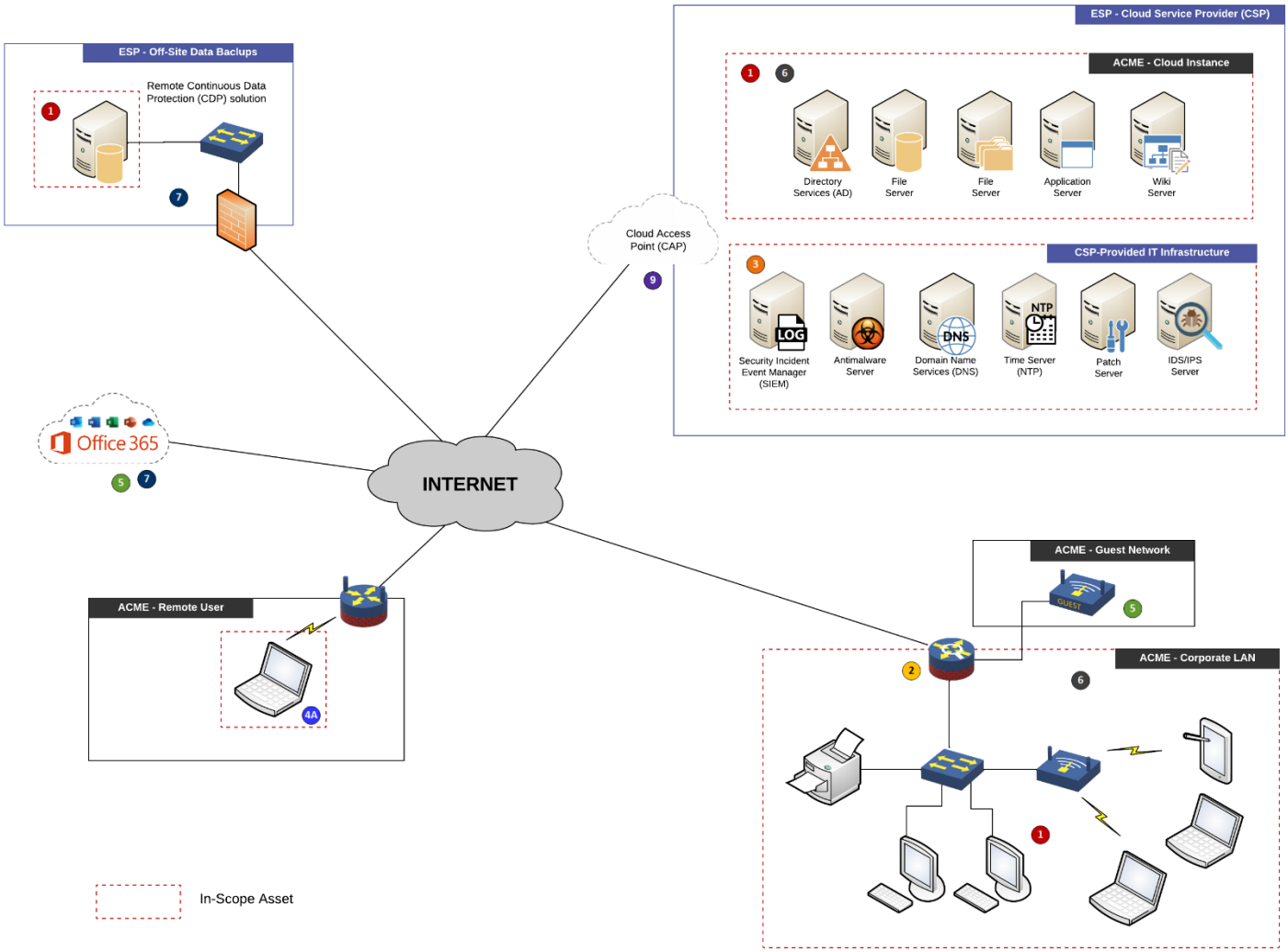
- Since ACME buys commercially available material and does not share CUI with its suppliers, they are out-of-scope (**zone 5**). **CMMC – OOSA**

SCENARIO 3: CUI ON A VIRTUAL NETWORK (CLOUD INFRASTRUCTURE)

In this scenario, ACME Staffing (ACME) is the Organization Seeking Assessment (OSA) 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 Controlled Unclassified Information (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 CMMC Level 2 organization, since it P/S/T 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 Microsoft Office365 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 2 assessment.

ORGANIZATIONS – CORPORATE LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**). **CMMC – OOSA**
- All IT assets on the organization's corporate LAN (wired & wireless) are in-scope either due to P/S/T CUI (**zone 1**) **CMMC – CUI Asset** or due to a lack of segmentation (**zone 4**). **CMMC – CRMA**
- ACME has a single firewall that connects to the Internet Service Provider (**ISP**) (**zone 2**). **CMMC – SPA**
- Email (Office365) is out of scope due to business practices prohibiting CUI from being emailed (**zones 5 & 7**). **CMMC – OOSA**

ORGANIZATIONS – 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 P/S/T CUI (**zone 1**) **CMMC – CUI Asset** or due to a lack of segmentation (**zone 4**). **CMMC – CRMA**

EXTERNAL SERVICE PROVIDER (ESP) - SECURE FILE TRANSFER SERVICE

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

CLOUD SERVICE PROVIDER (CSP)

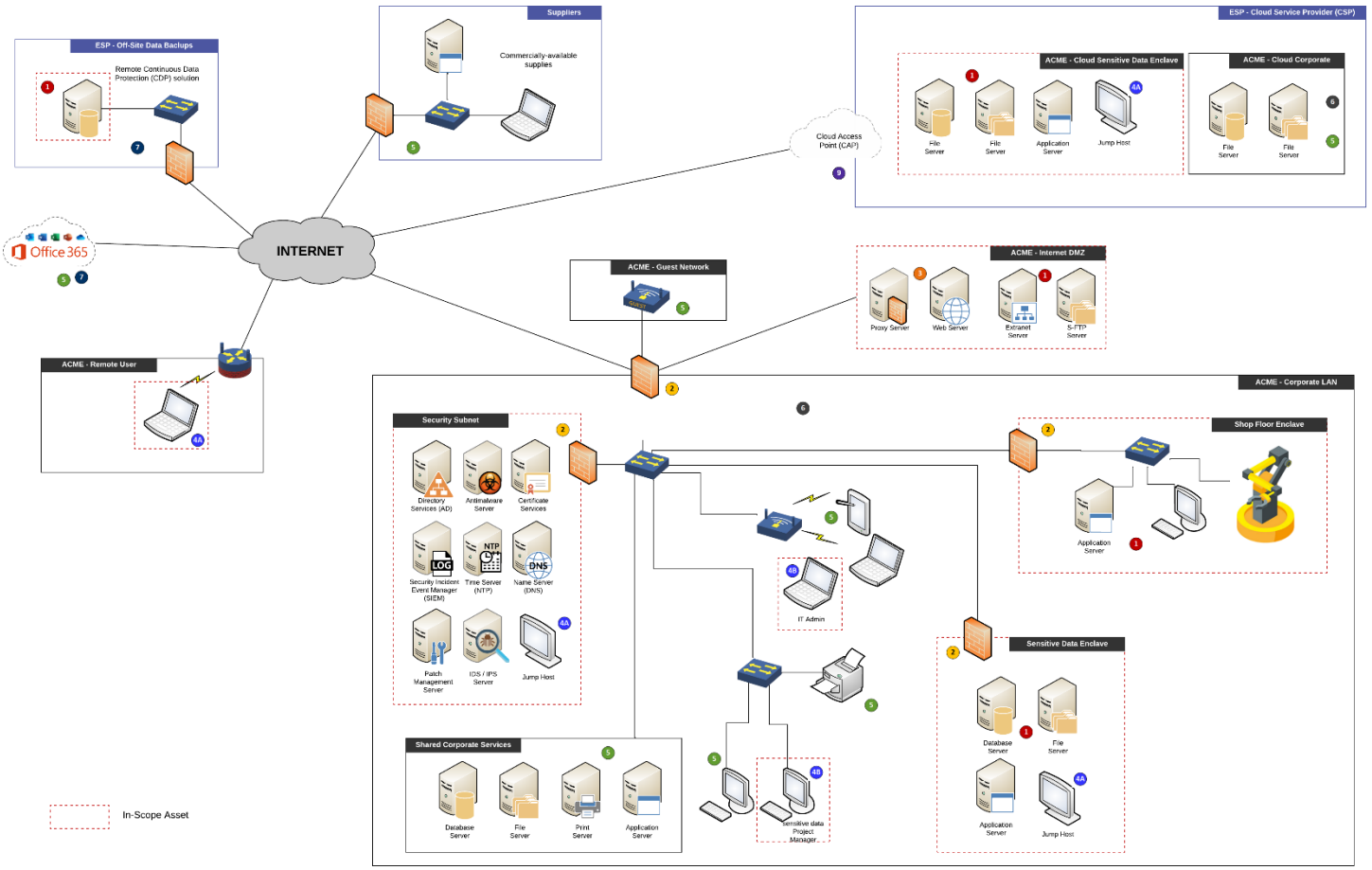
- Firewall rules to the CSP are in-scope (**zones 2 & 9**). **CMMC – SPA**
- All IT assets on the organization's cloud instance are in-scope either due to P/S/T CUI (**zone 1**) **CMMC – CUI Asset** or due to a lack of segmentation (**zone 4**). **CMMC – CRMA**
- CSP has a written contract with ACME that documents its security requirements (**zone 7**). CSP has a clearly-documented demarcation for the specific controls that it performs as part of its service offering. **CMMC – SPA**
- The "security tools" that protect both the organization's cloud instance are in-scope (**zone 3**). **CMMC – SPA** 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: CUI ON A HYBRID NETWORK (ON-PREMISE & CLOUD INFRASTRUCTURE)

In this scenario, ACME Engineering (ACME) is the Organization Seeking Assessment (OSA) and is a subcontractor on a project to develop components for a DoD weapons system. The components are categorized as Controlled Unclassified Information (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 CMMC Level 2 organization, since it P/S/T 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 2 assessment.

ORGANIZATIONS – CORPORATE LAN

- **Corporate LAN**
  - Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**). CMMC – OOSA
  - The majority of the organization's corporate LAN are out-of-scope (**zone 5**) due to segmentation. CMMC – OOSA
  - 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**). CMMC – CRMA
  - Email (Office 365) is out of scope due to business practices prohibiting CUI from being emailed (**zone 5**). CMMC – OOSA
- **CUI Enclave**
  - The firewall that provides segmentation services to sensitive/regulated data enclave is in scope (**zone 2**). CMMC – SPA
  - The database, file and application server all P/S/T CUI (**zone 1**). CMMC – CUI Asset
  - The jump host directly connects to zone 1 assets, so it is in scope (**zone 4a**). CMMC – CRMA
- **Shop Floor Enclave**
  - The firewall that provides segmentation services to the shop floor enclave is in scope (**zone 2**). CMMC – SPA
  - The application server P/S/T CUI (**zone 1**). CMMC – CUI Asset
  - The manufacturing workstation and CNC machines P/S/T CUI (**zone 1**). CMMC – OOSA & CMMC – SA
- **Security Subnet**
  - The firewall that provides segmentation services to the security subnet is in scope (**zone 2**). CMMC – SPA
  - The jump host directly connects to zone 3 assets, so it is in scope (**zone 4a**). CMMC – CRMA
  - The "security tools" that protect both the corporate LAN and enclave is in scope (**zone 3**). CMMC – SPA 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**). CMMC – OOSA

ORGANIZATIONS – INTERNET DMZ & GUEST NETWORK

- The Internet DMZ is in scope since it contains an extranet server that is used to P/S/T CUI (**zone 1**) CMMC – CUI Asset and the proxy server is in-scope (**zone 3**) CMMC – SPA since it provides security services.
- The "guest network" is segmented from the corporate LAN and is out-of-scope (**zone 5**). CMMC – OOSA

ORGANIZATIONS – REMOTE USER

- The remote users are not in scope (**zone 5**), since they do not have access to CUI. CMMC – OOSA
- 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**). CMMC – CRMA

ORGANIZATIONS – CORPORATE LAN

- Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**). CMMC – OOSA
- All IT assets on the organization's corporate LAN (wired & wireless) are in-scope either due to P/S/T CUI (**zone 1**) CMMC – CUI Asset or due to a lack of segmentation (**zone 4**). CMMC – CRMA
- ACME has a single firewall that connects to the Internet Service Provider (**ISP**) (**zone 2**). CMMC – SPA

EXTERNAL SERVICE PROVIDER (ESP) - SECURE FILE TRANSFER SERVICE

- Due to CUI being stored in the off-site backups, that takes that service within scope (**zone 1**). CMMC – CUI Asset
- ESP has a written contract with ACME that documents its security requirements (**zone 7**). CMMC – SPA

- The ESP is excluded from additional controls, since it has no access to the private key that encrypts the backed up data.
- The organizations must secure the secure file transfer service by implementing controls associated with access control and multifactor authentication to appropriately protect the data being housed offsite.

Cloud Service Provider (CSP)

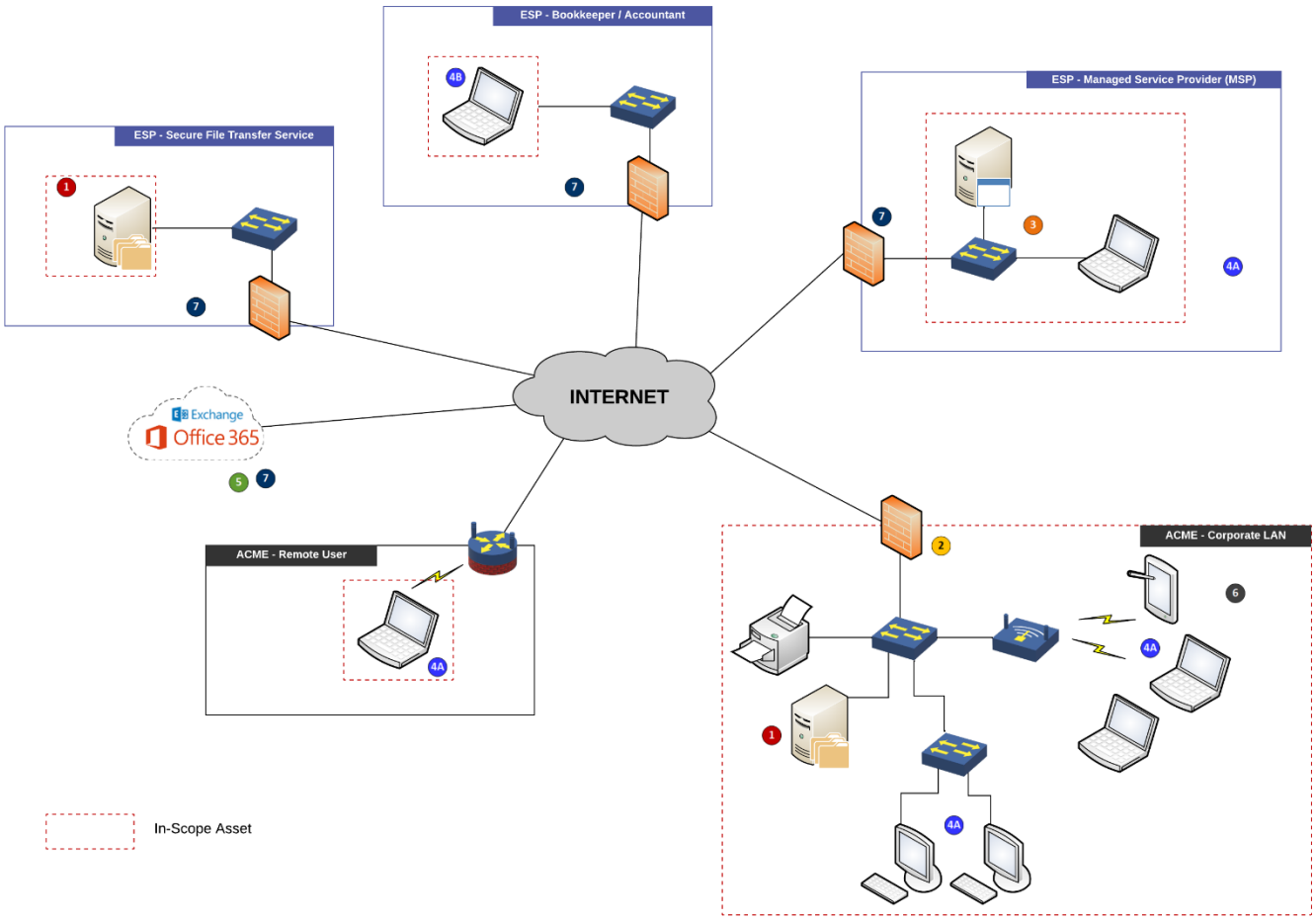
- Firewall rules to the CSP are in-scope (**zones 2 & 9**). **CMMC – SPA**
- The CUI enclave in the cloud instance is in-scope due to P/S/T CUI (**zones 1 & 9**) **CMMC – CUI Asset** and remote users needing access must connect to a "jump host" within that enclave (**zone 4a**). **CMMC – CRMA**
- The CUI enclave for corporate IT assets that do not contain CUI in the cloud instance is out-of-scope (**zone 5**). **CMMC – OOSA**
- CSP has a written contract with ACME that documents its security requirements (**zones 7 & 9**). **CMMC – SPA** CSP has a clearly-documented demarcation for the specific controls that it performs as part of its service offering.

SCENARIO 5: SENSITIVE IP & PD ON A FLAT NETWORK

In this scenario, ACME Consulting (ACME) is the organization and developed an application to better manage its internal operations that contains both sensitive IP (trade secrets) and PD of its employees and customers.

BACKGROUND SCENARIO DETAILS:

- While the IP is not regulated, the PD falls under EU GDPR & CCPA so there are cybersecurity & data privacy requirements.
- ACME defines its "secure practices" as alignment with the NIST Cybersecurity Framework (NIST CSF) and defines its "data privacy practices" as alignment with the NIST Privacy Framework.
- While ACME is not a large company, it has a global client base.
- While ACME is able to perform its core mission in-house, it does not have a dedicated IT, cybersecurity or administrative staff, so it relies on External Service Providers (ESP) for bookkeeping and technology support.
- ACME utilizes a "flat" network without dedicated subnets for sensitive/regulated data.
- ACME does have remote users who must connect via VPN to access corporate resources.
- ACME utilizes a secure file transfer service to send/receive sensitive/regulated data.
- ACME uses Office 365 for email but administratively prohibits sensitive/regulated data 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 the necessary cybersecurity and data protection controls to protect the IP and PD. 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 that would need to demonstrate equivalent cybersecurity and data protection practices (e.g., NIST CSF and NIST Privacy Framework controls).

ORGANIZATIONS – 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 sensitive/regulated data (**zone 1**).
- Several organizations users have sensitive/regulated data on their workstations (**zone 1**). However, the majority of the organization's users do not have sensitive/regulated data 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 sensitive/regulated data from being emailed (**zone 5**).

ORGANIZATIONS – 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 P/S/T sensitive/regulated data (**zone 4a**) and fall within scope.
- The "security tools" the MSP uses protect ACME's corporate LAN have direct access to devices that P/S/T sensitive/regulated data (**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 P/S/T sensitive/regulated data (**zone 4b**) and fall within scope.

SECURE FILE TRANSFER SERVICE

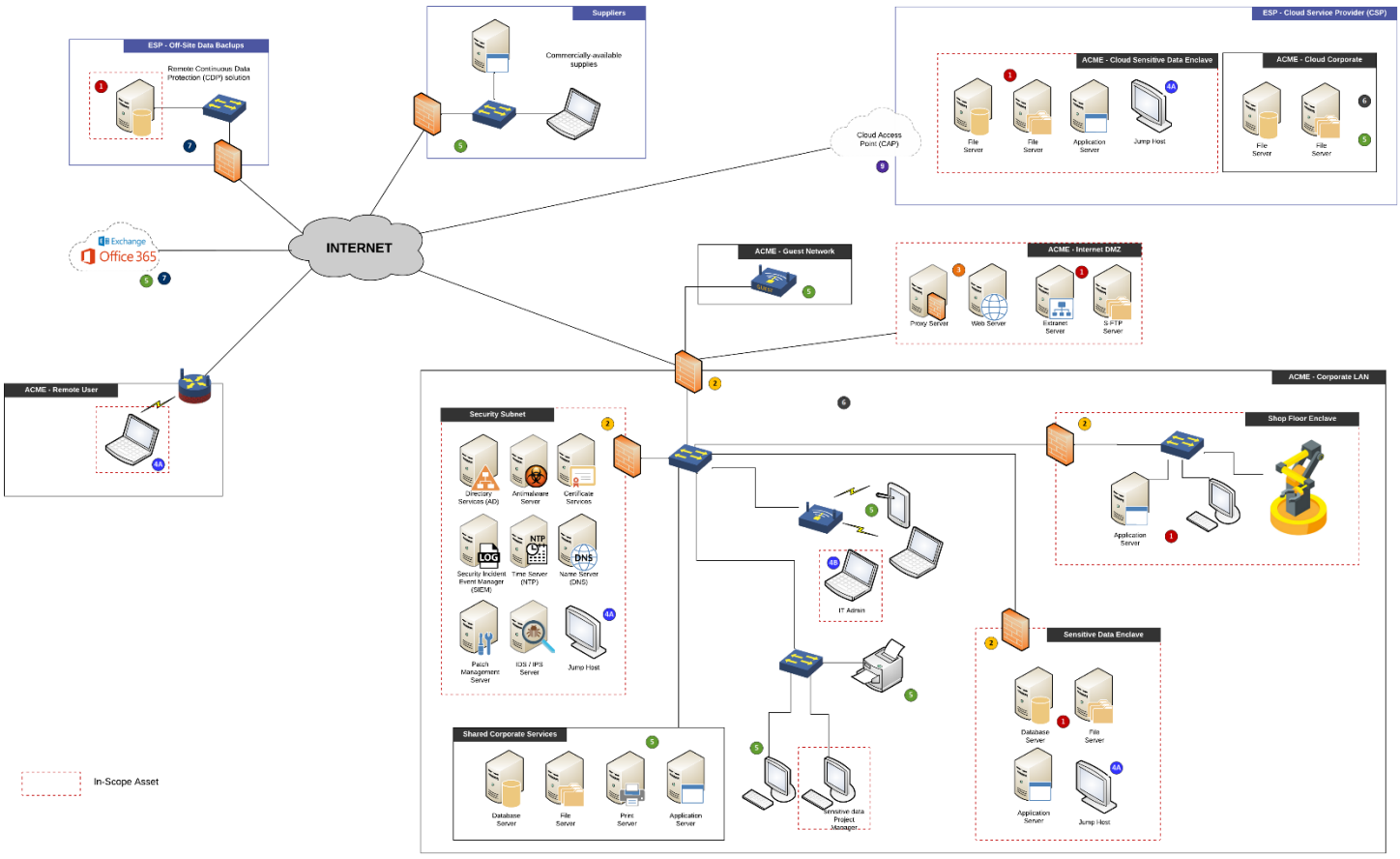
- Due to sensitive/regulated data being temporarily stored and transmitted in the file transfer service's systems, that takes that service within scope (**zone 1**). While sensitive/regulated data is encrypted in transit, applicable controls need to be reviewed and applied for instances where sensitive/regulated data 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 ESP 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 organizations must secure the secure file transfer service by implementing applicable controls associated with access control to appropriately protect the data being housed offsite.

SCENARIO 6: SENSITIVE IP & PD ON A SEGMENTED NETWORK

In this scenario, ACME Engineering (ACME) is the organization and is a subcontractor on a project to develop components of consumer electronic devices. The contract contains sensitive IP (client trade secrets) and the components contain sensors that process sensitive PD (sPD) of its employees and customers.

BACKGROUND SCENARIO DETAILS:

- While the IP is not regulated, the PD falls under EU GDPR & CCPA so there are cybersecurity & data privacy requirements.
- ACME defines its "secure practices" as alignment with the ISO 27001/27002 and defines its "data privacy practices" as alignment with the ISO 29100.
- ACME relies on subcontractors 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 sensitive/regulated data from being communicated by email.
- Within ACME's corporate LAN, there are three enclaves:
    4. A "security subnet" where it hosts security-related services for the entire organization;
    5. A specifically designed sensitive/regulated data enclave, where sensitive/regulated data is hosted to segment it from the rest of the network;
    6. 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 sensitive/regulated data.
- ACME uses several suppliers, but it does not share sensitive/regulated data 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 the necessary cybersecurity and data protection controls to protect the IP and sPD. Due to segmentation, only certain parts of ACME's network and select third-party services would need to demonstrate equivalent cybersecurity and data protection practices (e.g., ISO 27001/27002 and ISO 29100 controls).

ORGANIZATIONS – CORPORATE LAN

- **Corporate LAN**
  - Organization-wide security practices apply (e.g., corporate policies) apply to the corporate LAN (**zone 6**).
  - The majority of the organization's corporate LAN (wired & wireless) are out-of-scope (**zone 5**) due to segmentation.
  - Corporate users needing access into a subnet that contains sensitive/regulated data 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 sensitive/regulated data from being emailed (**zone 5**).
- **Sensitive Data Enclave**
  - The firewall that provides segmentation services to sensitive/regulated data enclave is in scope (**zone 2**).
  - The database, file and application server all P/S/T sensitive/regulated data (**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 P/S/T sensitive/regulated data (**zone 1**).
  - The manufacturing workstation and CNC machines P/S/T sensitive/regulated data (**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-sensitive/regulated data servers, print servers and application servers that are not in-scope (**zone 5**).

ORGANIZATIONS – INTERNET DMZ & GUEST NETWORK

- The Internet DMZ is in scope since it contains an extranet server that is used to P/S/T sensitive/regulated data (**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**).

ORGANIZATIONS – REMOTE USER

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

EXTERNAL SERVICE PROVIDER (ESP) - SECURE FILE TRANSFER SERVICE

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

SUPPLIERS

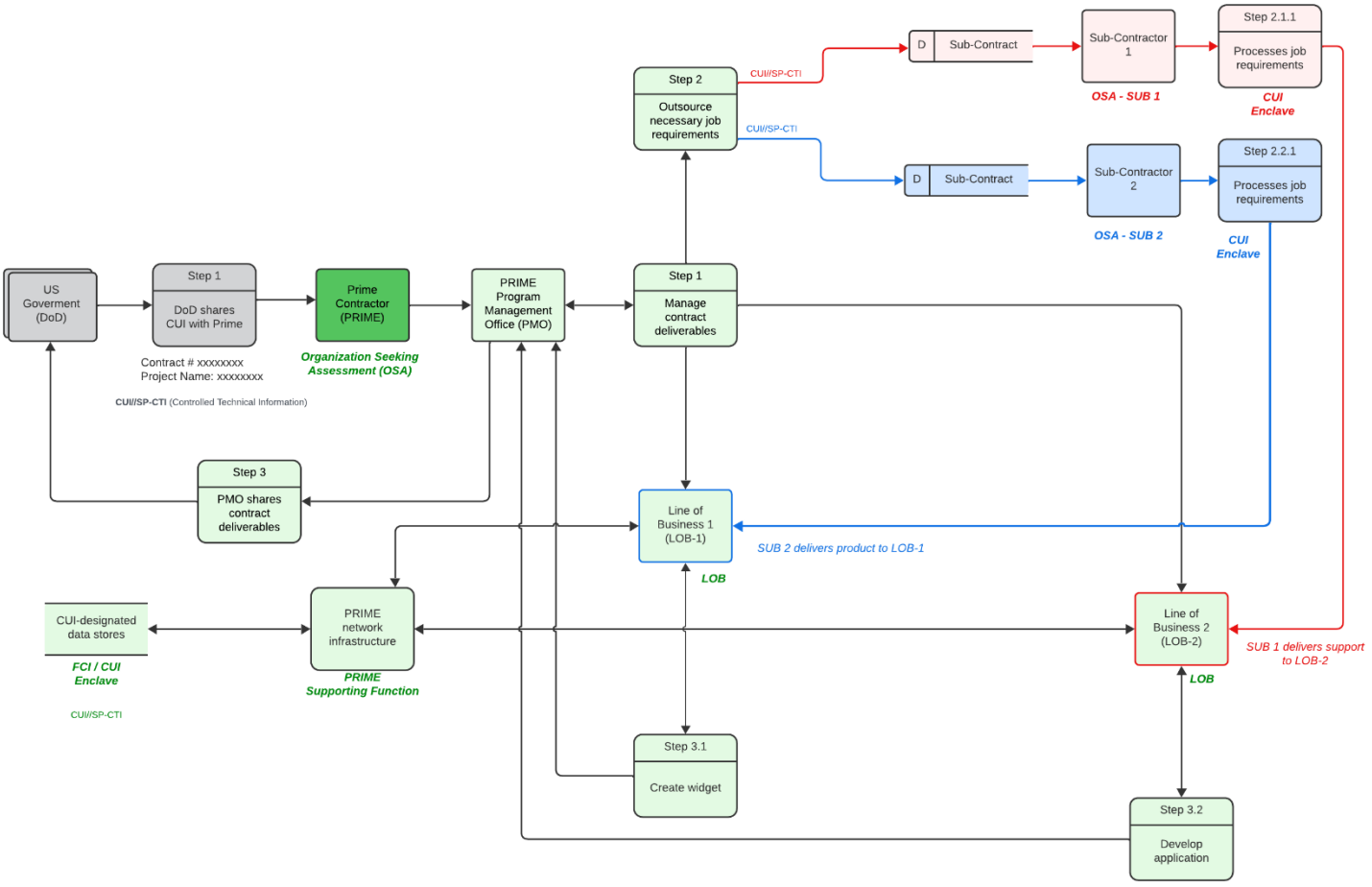
- Since ACME buys commercially available material and does not share sensitive/regulated data with its suppliers, they are out-of-scope (**zone 5**).

Cloud Service Provider (CSP)

- Firewall rules to the CSP are in-scope (**zone 2**).
- The sensitive/regulated data enclave in the cloud instance is in-scope due to P/S/T sensitive/regulated data (**zone 1**) and remote users needing access must connect to a "jump host" within that enclave (**zone 4a**).
- The sensitive/regulated data enclave for corporate IT assets that do not contain sensitive/regulated data 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 controls that it performs as part of its service offering.

APPENDIX A: EXAMPLE DATA FLOW DIAGRAM (DFD) FOR CUI

A Data Flow Diagram (DFD) maps out the flow of information for any process (including information flow between systems). For compliance concerns such as NIST SP 800-171 and CMMC, having a DFD is very important.



As part of a DFD, it is necessary to identify the key stakeholders and their processes that P/S/T in-scope data:

- **Organization Seeking Assessment (OSA)**: The legal entity that is engaged in a contract/grant with the U.S. Government that is in-scope for CMMC certification either as a prime or sub-contractor.
  - An organization may be defined in part by a Commercial and Government Entity (CAGE) code, which is required to support any Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR) contract/grant.
  - An organization may be a Foreign Ownership, Control or Influence (FOCI) mitigated entity.
- **Line of Business (LOB)**: The department within the organization that is primarily responsible for the contract that contains sensitive/regulated data.
  - A single LOB may have multiple in-scope contracts.
  - Large and/or complex organizations might have a LOB within a LOB (e.g., be organized with multiple layers of LOBs).
- **Organization Shared Services**: Any other function/department that operates across multiple LOBs within the organization is in-scope due to:
  - Data mingling (e.g., server infrastructure, network subnets, etc.); and/or
  - Technology dependencies (e.g., SOC, NOC, directory services, DNS, NTP, etc.).
- **External Service Provider (ESP)**: Any third-party that provides services to the organization.
  - An ESP operates across organizations (multiple legal entities).
  - The "flow down" requirements for sensitive/regulated data must be addressed with each ESP to clearly identify the ESPs' roles and responsibilities associated with sensitive/regulated data, if applicable.
  - A shared service between a conglomerated business, where each business is an independent legal entity, would

be considered a third-party relationship where the subsidiary/business entity providing the service (e.g., IT, legal, finance, etc.) would be considered an ESP.
    - Conglomerated businesses would be expected to have multiple CMMC assessments, where each in-scope subsidiary/business entity would be an organization.
    - The C3PAO would be able to leverage a passing CMMC assessment to cover the applicable CMMC practices/processes provided by the shared services among the conglomerated business.
- **Sensitive Data Enclave**: A sub-network that is logically or physically separated from the rest of the network.
    - The sensitive/regulated data environment exists as an enclave, separate from the rest of the organization's networks, to protect the confidentiality and integrity of sensitive/regulated data (e.g., manufacturing shop floor enclave, project lab enclave, project management office enclave, etc.).
    - The sensitive/regulated data Enclave may inherit security controls from the organization.

APPENDIX B: SCOPING CONSIDERATIONS FOR VIRTUAL DESKTOP INFRASTRUCTURE (VDI)

There are several topical issues that compel a more thorough discussion on VDI:

- Remote workforce requirements (e.g., work from home);
- Bring Your Own Device (BYOD) security concerns; and
- Cybersecurity Maturity Model Certification (CMMC) and NIST SP 800-171 compliance efforts to minimize scoping.

The end goal is for an organization to be both secure and compliant.

- For organizations that are unregulated, where there are no statutory, regulatory or contractual obligations for data protection, the discussion is more focused on (1) security, (2) user functionality and (3) cost.
- For organizations that have data protection obligations, there is added criteria to evaluate how VDI affects scoping.

32 CFR Part 170 Guidance for CMMC & NIST SP 800-171 Compliance

Per 32 CFR Part 170, endpoint client devices are considered out-of-scope when VDI is configured to:

- Enable only client Keyboard, Video, Mouse (KVM) functionality; and
- Prevent P/S/T of CUI on the end client.

Benefits of VDI

The expressed benefits of VDI include, but are not limited to:

- Increased security
- Cost savings
- Centralized management
- Managed remote access

There are several excellent writeups on the benefits of VDI from leading solutions providers:

- VMware; [47] and
- Microsoft[48]

Drawbacks of VDI

With how VDI works, the endpoint (e.g., remote PC, BYOD, etc.) is actually "processing and transmitting" sensitive/regulated data when that information is displayed on the endpoint, either within an application or browser. For both managed or unmanaged endpoints, the sensitive/regulated data temporarily exists in the CPU and RAM while the information is being displayed. By P/S/T sensitive/regulated data, the endpoint would be considered to be within scope for the applicable data protection controls.

VDI that allows access to sensitive information may be considered one of the two in-scope categories:

- Zone 1: Any system, application and/or service that P/S/T sensitive/regulated data. These systems that interact with sensitive/regulated data are the main assets that sensitive/regulated data are trying to protect.

- Zone 4: VDI that interacts with Zone 1 assets would be considered a Zone 4 asset, which is any system that has some capability to communicate with systems, applications or services within the sensitive/regulated data environment. A "connected" system, embedded technologies, application or service should be considered in scope for since it is not completely isolated. If it can potentially impact the security of sensitive/regulated data, it is in scope.

If you look at "industry recognized practices" for scoping sensitive/regulated data, the PCI Security Standards Council (**PCI SSC**) has published extensive guidance documentation on the subject. The following is quote from the PCI SSC's *Navigating PCI DSS: Understanding the Intent of the Requirements*[49] document:

---

[47] *VMware - https://www.vmware.com/topics/glossary/content/virtual-desktop-infrastructure-vdi*
[48] *Microsoft - https://azure.microsoft.com/en-us/free/services/virtual-desktop/*
[49] *PCI SSC Navigating PCI DSS: Understanding the Intent of the Requirements - https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf*

> *"If virtualization is implemented, all components within the virtual environment will need to be identified and considered in scope for the review, including the individual virtual hosts or devices, guest machines, applications, management interfaces, central management consoles, hypervisors, etc. All intra-host communications and data flows must be identified and documented, as well as those between the virtual component and other system components.*
>
> *The implementation of a virtualized environment must meet the intent of all requirements, such that the virtualized systems can effectively be regarded as separate hardware. For example, there must be a clear segmentation of functions and segregation of networks with different security levels; segmentation should prevent the sharing of production and test/development environments; the virtual configuration must be secured such that vulnerabilities in one function cannot impact the security of other functions; and attached devices, such as USB/serial devices, should not be accessible by all virtual instances."*

As explained in the PCI SSC's *Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* document pertaining to the scope of PCI DSS requirements: [50]

> *The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that P/S/T cardholder data or sensitive authentication data.*

VMware provides additional guidance on segmentation considerations for virtualized environments.[51]

Workarounds

Determining options for VDI being considered in-scope depends on the specific statutory, regulatory and/or contractual obligation, so there is no blanket answer for how to address in-scope VDI.

If compensating controls are an option (e.g., PCI DSS, FedRAMP, etc.):

- From a technical perspective:
  - Geofencing to limit the acceptable locations where VDI can be accessed;
  - Day/time limitations for accessing VDI; and/or
  - Restrictive security configurations that prevent:
    - Copying (including screen capture);
    - Printing; and
    - Saving to the end device.
- There are a few non-technical, administrative controls to prevent the abuse of sensitive/regulated data that is displayed and temporarily processed in a VDI session:
  - Requiring users to attest to rules of behavior;
  - Designating acceptable and unacceptable physical locations to access VDI; and
  - Role-based security training.

---

[50] *PCI SSC Information Supplement: Guidance for PCI DSS Scoping and Network Segmentation* https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

[51] *VMware Solution Guide for Payment Card Industry* - https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/vmware-payment-card-industry-solution-guide.pdf

APPENDIX C: DEFINING "MUST HAVE" VS "NICE TO HAVE" SECURITY CONTROLS

The Integrated Controls Management (ICM) is a free resource for businesses to help identify their "must have" vs "nice to have" security controls.[52]

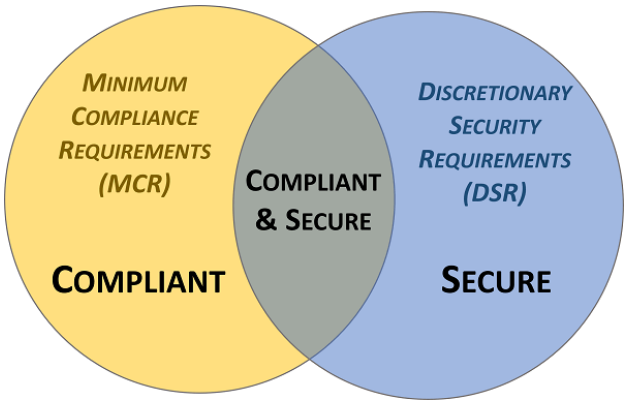
The ICM is defined as, *"a holistic, technology-agnostic approach to cybersecurity and data protection controls to identify, implement and manage secure and compliant practices, covering an organization's people, processes, technology and data, regardless of how or where data is P/S/T."*

In practical terms, controls exist to protect an organization's data. Requirements for asset management do not primarily exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but data residing on those devices cannot. This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity & data protection program, since it provides guidelines to establish the scope for control applicability. The ICM assists in this process.

Similar in concept to Governance, Risk & Compliance (GRC) or Integrated Risk Management (IRM), ICM is focused on supporting processes and practices that must exist for a cybersecurity & data protection program to operate effectively and efficiently. ICM is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity & data protection program.

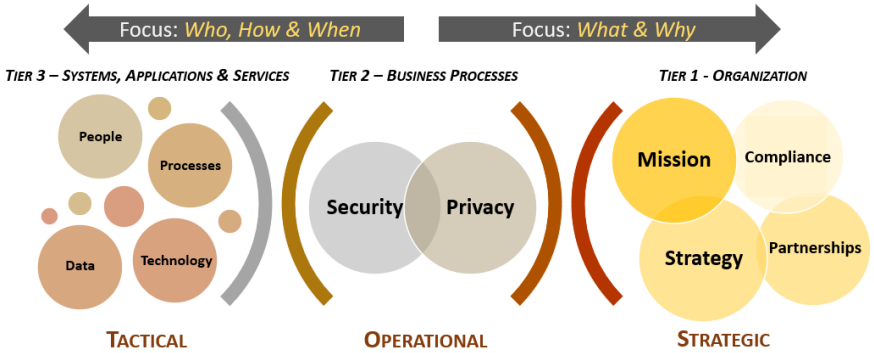
Unlike GRC/IRM, ICM specifically focuses on the need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, ICM helps an organization categorize its applicable controls according to "must have" vs "nice to have" requirements:

- **Minimum Compliance Requirements (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- **Discretionary Security Requirements (DSR)** are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.



[52] *ICM - https://complianceforge.com/content/pdf/complianceforge-integrated-controls-management.pdf*

APPENDIX D: DOCUMENTATION TO SUPPORT CYBERSECURITY & DATA PROTECTION

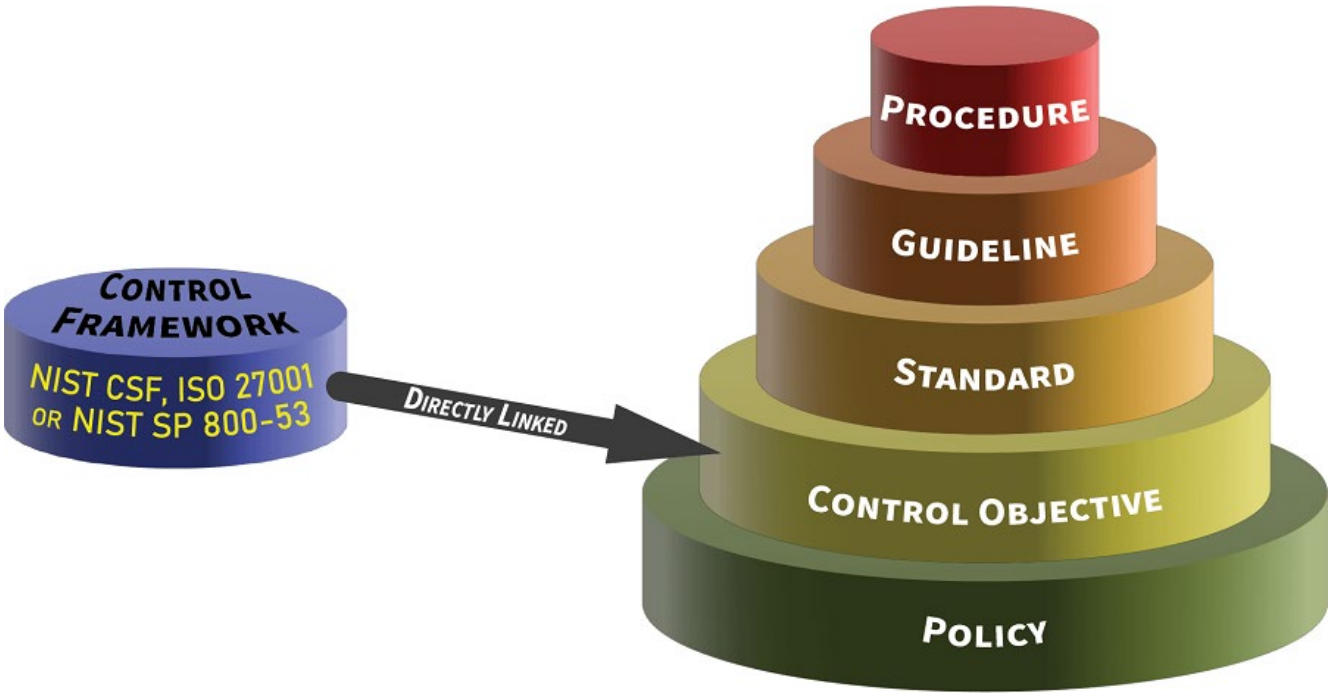
The purpose of a company's cybersecurity documentation is to prescribe a comprehensive framework for:

- 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:

In the context of good cybersecurity documentation, components are hierarchical and build on each other to build a strong governance structure that utilizes an integrated approach to managing requirements. Well-designed documentation is generally comprised of six (6) main parts:

1. Policies establish management's intent;
2. Control Objectives identify leading practices (mapped to requirements from laws, regulations and frameworks);
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met (requirements from laws, regulations and frameworks);
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.



When that is all laid out properly, your company's cybersecurity documentation should flow from policies all the way down to metrics. This is further explained in ComplianceForge's Hierarchical Cybersecurity Governance Framework (HCGF).[53]

[53] *HCGF - https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf*