

CMMC 2.0 Level 2 Scoping Tree

version 2023.1



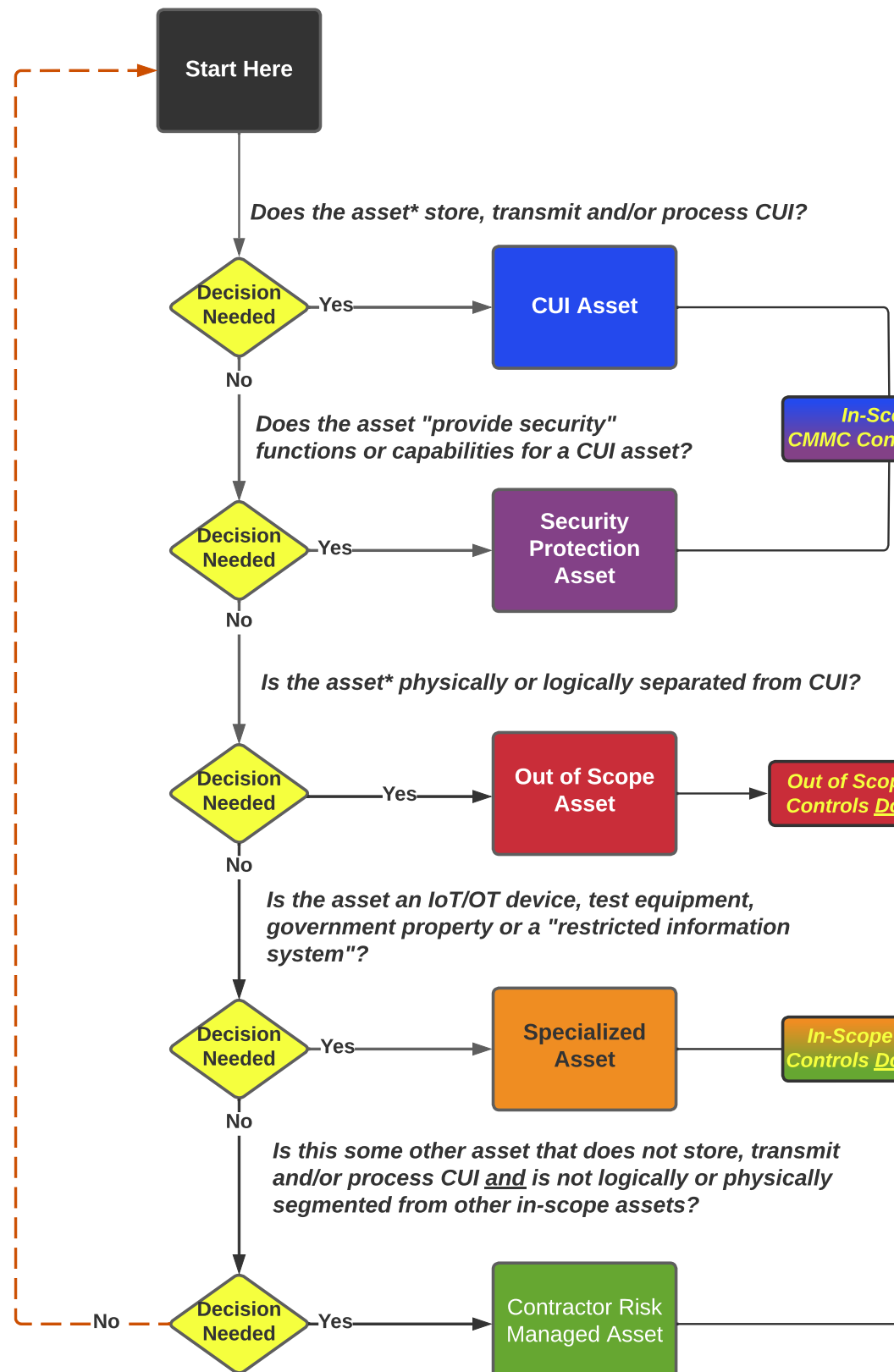
www.CMMC-COA.com

Attribution-NoDerivatives 4.0 International



If you are looking for a scoping guide that addresses FCI & CUI, but can do a lot more, then check out the FREE Unified Scoping Guide (USG) that provides a zone-based model to apply a data-centric security approach for scoping sensitive & regulated data

Unified Scoping Guide
Sensitive & Regulated Data
<https://www.unified-scoping-guide.com>



If you answered NO then you made a mistake and need to start the scoping process again.

CMMC-Specific

Policies, Standards & Procedures

CMMC-specific policies, standards and procedures are applicable to the system, application, service, person or External Service Provider (ESP).

Realistically, CMMC-specific documentation (e.g., policies, standards and procedures) should be a subset of the organization's overall Governance, Risk & Compliance (GRC) scope for policies, standards and procedures.

In this case, CMMC-specific requirements would only be applicable to those specific assets that require the use of CMMC controls to protect CUI

DOCUMENTATION: ENTERPRISE ≥ CMMC

Enterprise-Wide**

Policies, Standards & Procedures

**** Enterprise Wide policies, standards and procedures are applicable to the OSC's systems, applications, services, people and External Service Providers (ESPs) that are not specifically covered by CMMC-specific policies, standards and procedures for CUI Assets and Security Protection Assets (SPAs).**

What this means is:

- Out of Scope Assets (OSAs), Contractor Risk Managed Assets (CRMA) and Specialized Assets (SA) need to be appropriately governed by the organization's non-CMMC- specific policies, standards and procedures.
- Per the CMMC L2 scoping guide, CRMA and SA are in-scope, but not subject to CMMC controls. The guide specifically calls out that contractors are required to "show [assets] are managed using the contractor's risk- based security policies, procedures, and practices."

The OSC's non-CMMC specific policies, standards and procedures are applicable to governing those CRMA and SA, even though they are in-scope to CMMC. Enterprise-level policies, standards and procedures provide "reasonable security" for CRMAs and SAs, but not SPAs or CUI Assets.

- CUI Asset
- Security Protection Asset (SPA)
- Contractor Risk Managed Asset (CRMA)
- Specialized Asset (SA)
- Out of Scope Asset (OSA)

Process - CUI can be used by an asset (e.g., accessed, entered, edited, generated, manipulated or printed)

Store - CUI is inactive or at rest on an asset (e.g., located on electric media, in system component memory or in physical format such as paper documents).

Transmit - CUI is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods).

*Definition: "asset" per CMMC Asset Scope - Level 2 guide

Asset Type	Security Protection Asset Examples
People	<ul style="list-style-type: none"> • Consultants who provide cybersecurity service • Managed service provider personnel who perform system maintenance • Enterprise network administrators
Technology	<ul style="list-style-type: none"> • Cloud-based security solutions • Hosted Virtual Private Network (VPN) services • SIEM solutions
Facility	<ul style="list-style-type: none"> • Co-located data centers • Security Operations Centers (SOCs) • Contractor office buildings