CMMC 2.0 L2 Scoping Tree

version 2024.4

- Cloud Service Provider (**CSP**)
- External Service Provider (**ESP**)
- CUI Asset
- Security Protection Asset (**SPA**)
- Specialized Asset (**SA**)
- Out of Scope Asset (**OOSA**)
- Contractor Risk Managed Asset (**CRMA**)

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://unified-scoping-guide

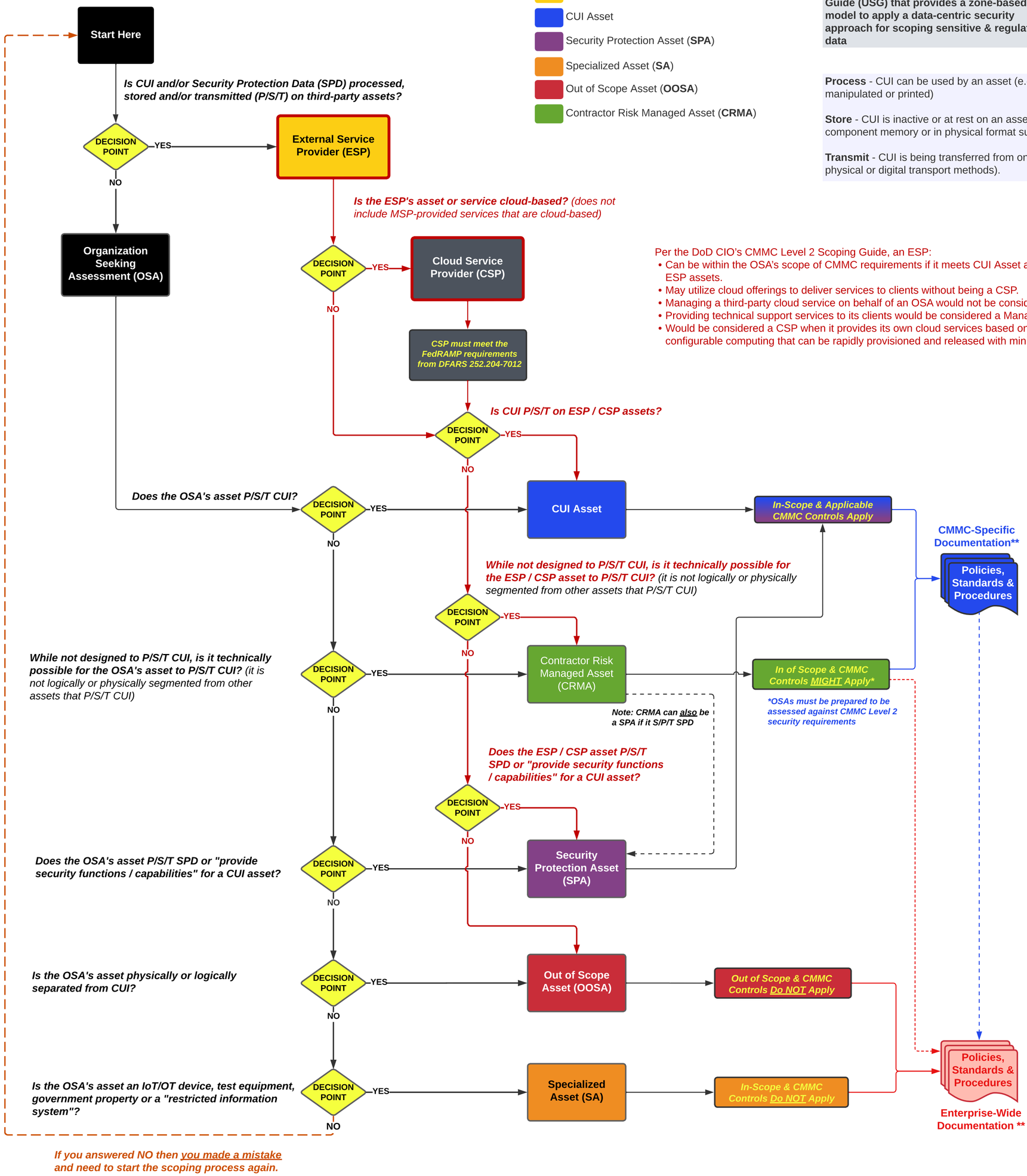
CMMC AWESOMENESS!

www.CMMC-COA.com

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).



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

- 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.

**** CMMC Documentation Considerations**

Enterprise-wide policies, standards and procedures are applicable to the OSA's People, Processes, Technologies, Data & Facilities (PPTDF), including ESP and CSP through contractual obligations. CMMC-specific compliance documentation should be a subset of the organization's broader documentation, where it is tailored for CMMC, but subordinate to the organization's broader cybersecurity policies, standards and procedures. The process of tailoring organization-wide requirements for CMMC involves specifying the applicability of standards and procedures to address CMMC requirements, so those CMMC requirements would only be applicable to the specific assets that require the use of CMMC controls to protect CUI.

The following entities need to be governed according to the OSA's Cybersecurity Supply Chain Risk Management Plan (C-SCRM Plan):

- External Service Providers (ESP); and
- Cloud Service Providers (CSP).

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:

- 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:
  - 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.**