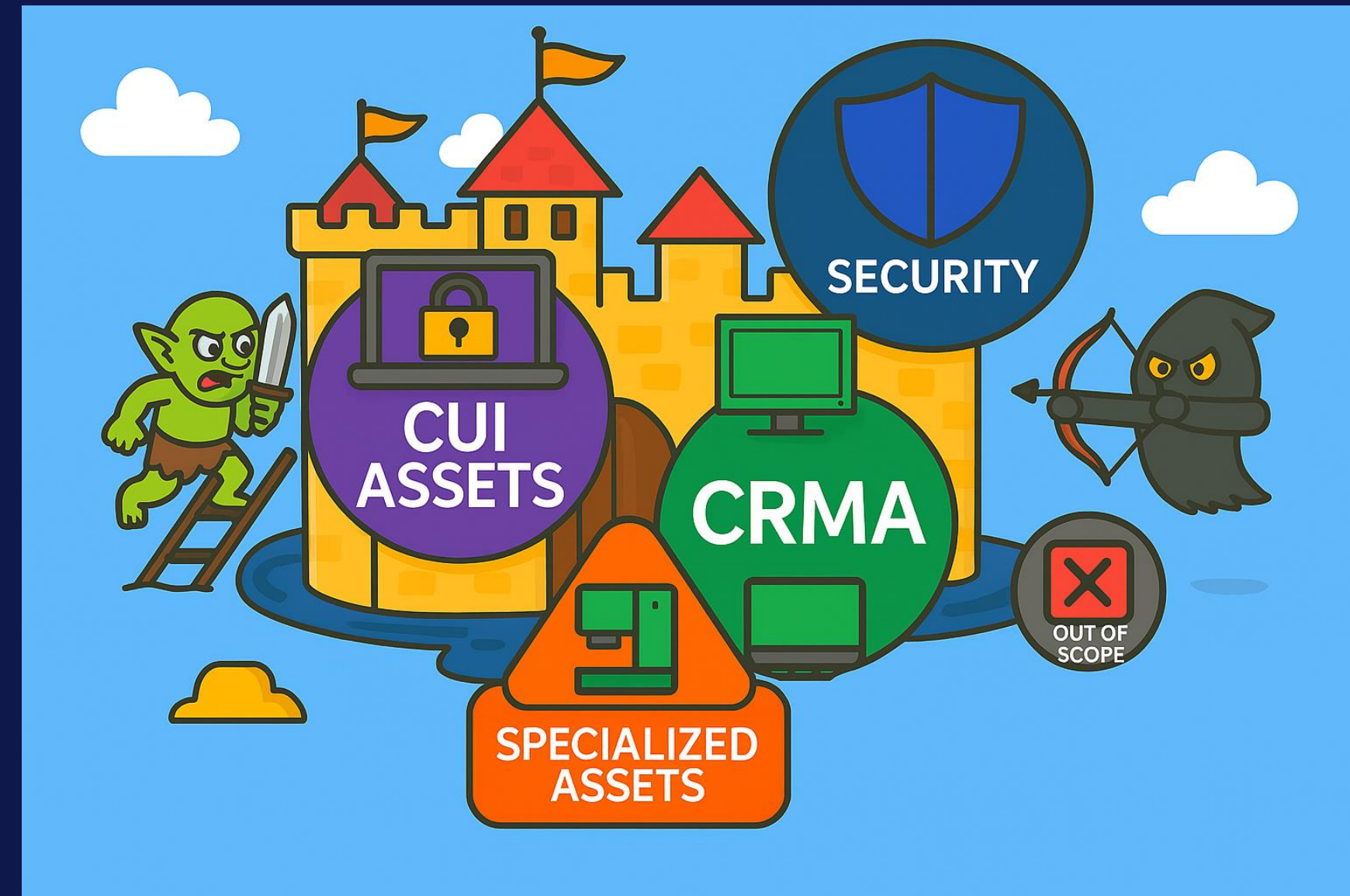


Know Your Boundary

Scoping MSP Services for CMMC Compliance

Ace Swerling
CompliancyIT

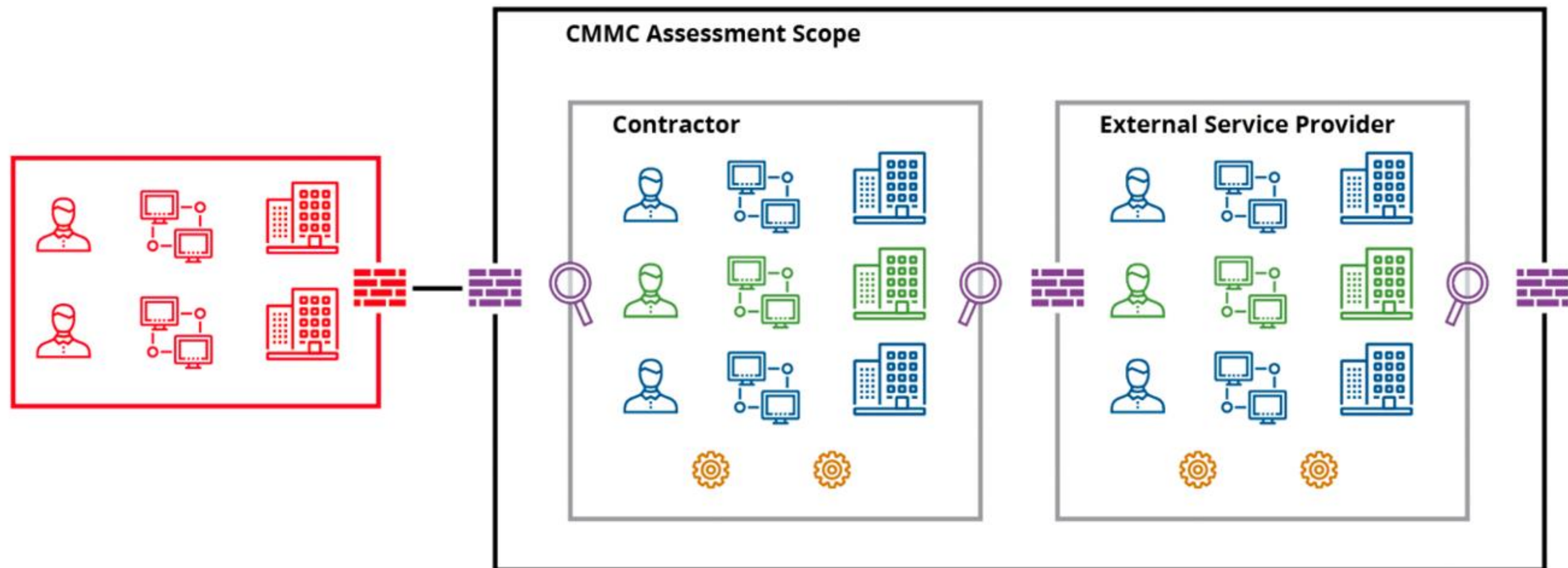


What Is Scoping?

- BLUF (bottom line up front) – this is what you are telling the assessor to assess
- Involves understanding how CUI enters your organization, what you do with it and where it goes
- Sometimes it is easier to figure out where CUI is *not* in your organization (think HR and Finance)
- It's not just IT systems, remember to include buildings, paper, and people for the OSC and all ESPs
- The scope defines what's inside the boundary

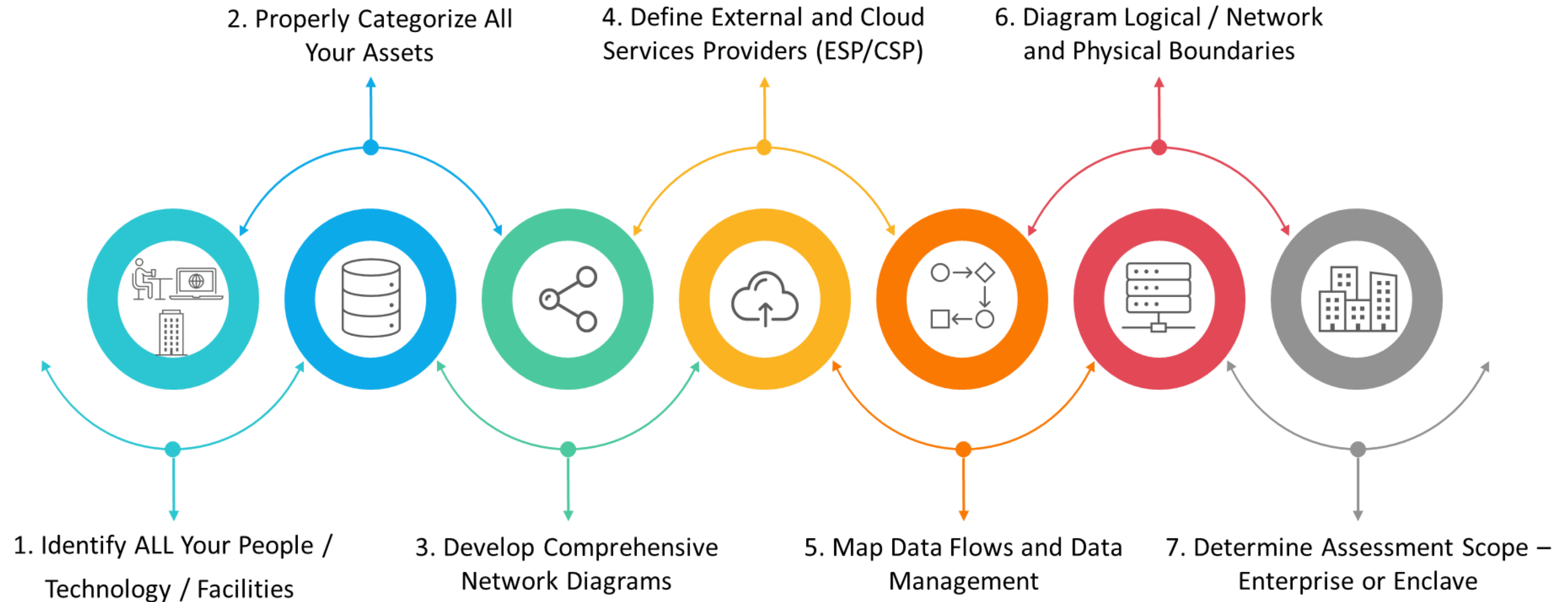
CUI Assets	Assets that process, store, or transmit CUI
Security Protection Assets	Assets that provide security functions or capabilities
Specialized Assets	Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment
Contractor Risk Managed Assets	Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
Out-of-Scope Assets	Assets that cannot process, store, or transmit CUI, do not provide security, and are logically or physically isolated from assets that do.

Example CMMC Assessment Scope



- CUI Assets
- Security Protection Assets
- Contractor Risk Managed Assets
- Specialized Assets
- Out-of-Scope Assets

Steps To Scope The Boundary



• Credit to Mark DeBry and Koren Wise

This Matters Because...



A Lot Of Stuff Is In Scope

- All Assets that store, process, or transmit CUI
- Everything that supports these processes
- This includes ESP services

This Much Stuff Breeds Complexity

- Reducing scope can simplify compliance, but everything still must be included
- ESPs are assessed alongside OSAs
- ESP CMMC certification enables inheritance, which streamlines assessment
- Still not a free pass

Complexity = 'It Depends'

- Expertise and experience is valuable to work through this.
- Consider business, risk, cost, user productivity, security, compliance

Scoping Has to Be Right. If Not, Contractors Are Vulnerable to False Claims Act

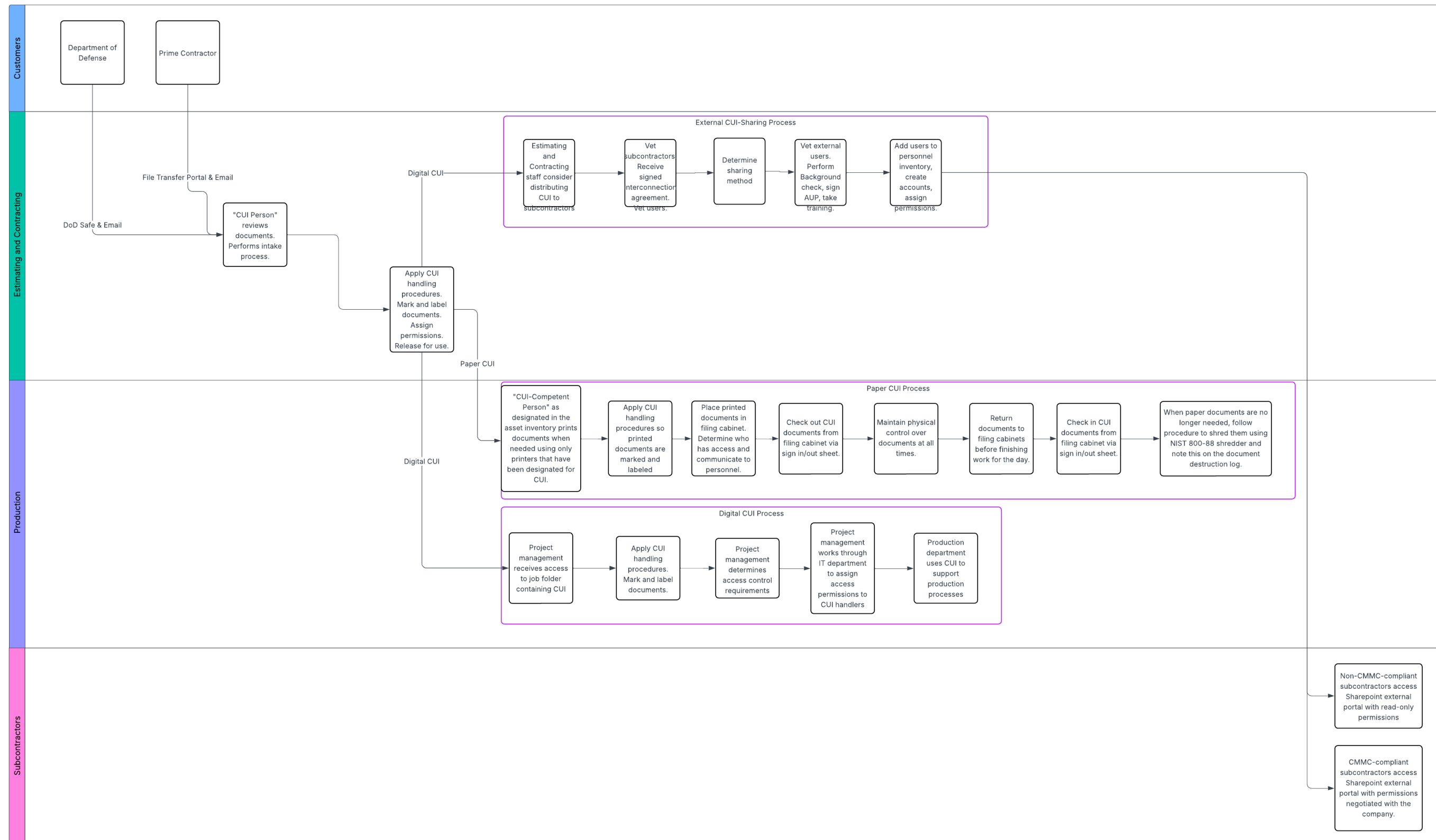
ESPs in Scope



Be Prepared For Your Clients' Assessments

- You're in scope as an External Service Provider ESP if you're providing support for an organizations' controls compliance.
 - An ESP can be an MSP, MSSP, or a CSP
- MSPs and MSSPs can be CMMC certified. If not, all your processes will be assessed alongside your clients'.
 - Have all your answers, documentation, and evidence ready. Demonstrate you're following procedures.
- CSPs provide cloud services as defined by NIST 800-145
 - "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction."
 - Must be FedRAMPed. Refer to CRM.
 - Be careful not to be a CSP if you want to be an MSP
 - See [September 2025 Town Hall – CyberAB](#) for more information

Start With Data Flow



Why Enclave?



The existing IT environment is terrible, and you need something else RIGHT NOW!

You're a big company and there's no way everything can be in scope for CMMC

You have a small number or percentage of users who need to access CUI

You have a capable IT department that knows how to run multiple environments

Business processes can support controlled data isolation without a productivity hit

Users work only with controlled data or only with uncontrolled data

You don't want to buy expensive SaaS licenses for everybody

Why Not Enclave?



Enclaves can cost a little less to implement and certify but multiple computing environments are more expensive in the long run

Small companies struggle to run one computing environment, let alone multiple

Companies need to secure their own data too. A little more cost can cover all data.

FCI, CUI, and other data are comingled and can't be easily separated *OR* the OSC doesn't know what their CUI is

Segregating controlled data to an enclave breaks business processes

What's the plan for FCI?

Scoping Wildcards

Printers

SaaS, IaaS, PaaS

- It is FedRAMPed?
- Can you get a CRM?

Security Protection Assets

- Does the vendor provide a CRM?
- How to handle SPAs outside the OSC's boundary?

Test systems, IoT, and specialized assets

AI

Authorized and unauthorized users in the same environment

Supply chain

- Sharing information with partners and suppliers
- Managing subcontractor compliance

Virtual desktops

Are you a CSP?

Setting Client Expectations

You can't do everything for your clients. They must follow procedures and make risk decisions.

CMMC isn't 'one and done.' It's an ongoing program that requires care and feeding.

Support must go through the ticketing system. Changes must go through Change Management.

CRMs are critical to define who's doing what. If you're working with another MSP or MSSP, make sure everything is covered.

Yes, you really do need to pay more for the FedRAMP version.

If an organization wants to add a CRM Asset later (like a SaaS containing CUI), make sure it's secured and documented beforehand. If not, the org just fell out of compliance.