



A Non-Technical Guide to CMMC Scoping

Presented by:
Ace Swerling
CompliancyIT





What Is Scoping?

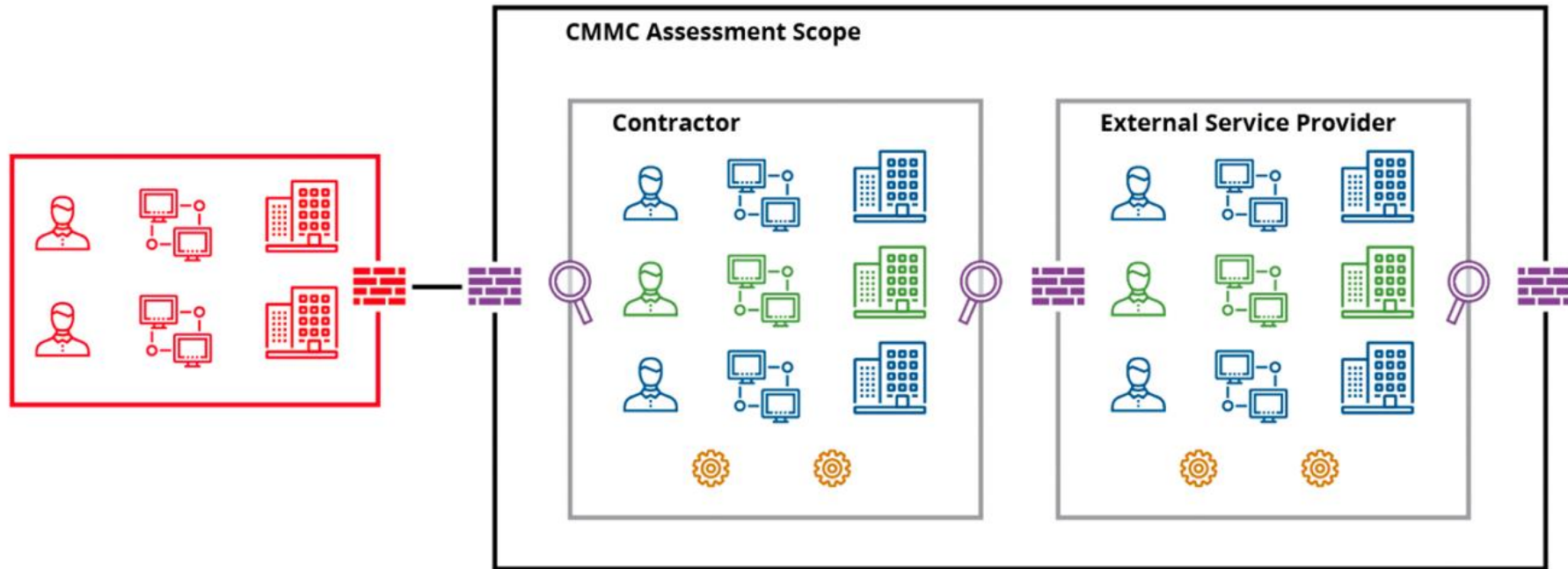
- BLUF (bottom line up front) – this is what you are telling the assessor to assess
- Involves understanding how CUI enters your organization, what you do with it and where it goes
- Sometimes it is easier to figure out where CUI is *not* in your organization (think HR and Finance)
- It's not just IT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

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

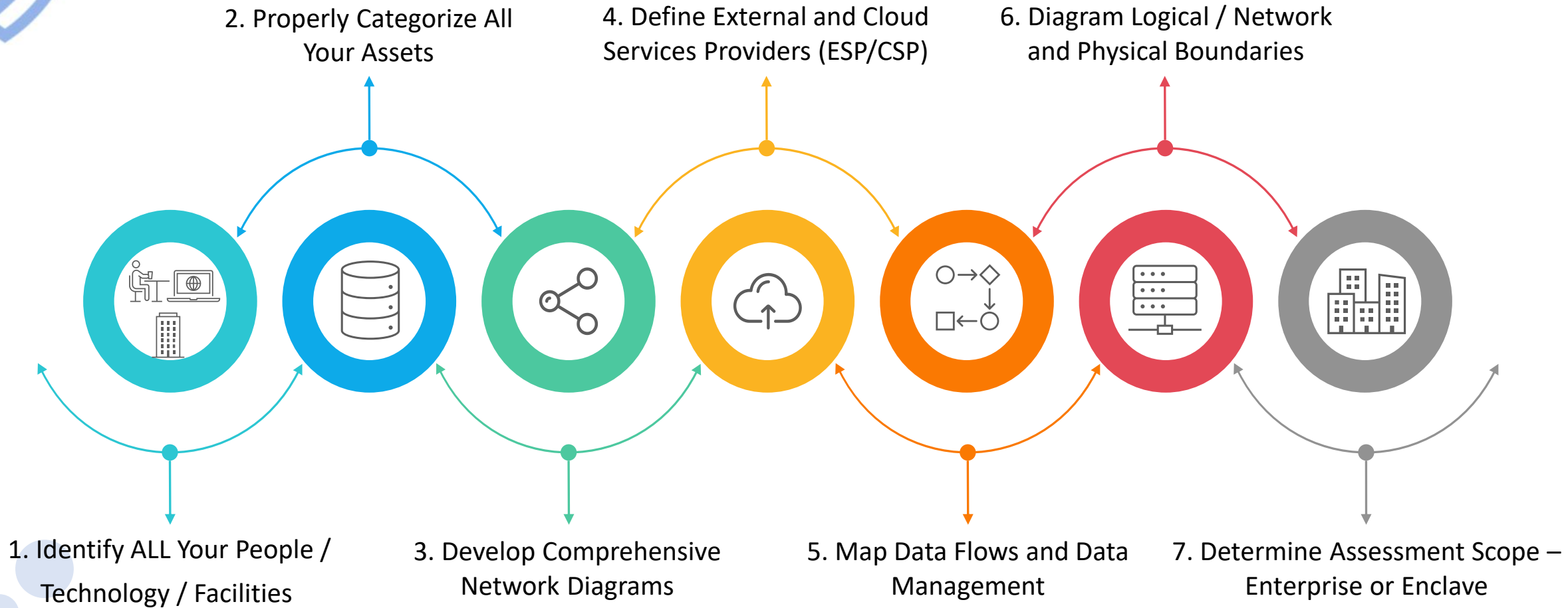


- CUI Assets
- Security Protection Assets
- Contractor Risk Managed Assets
- Specialized Assets
- Out-of-Scope Assets

• CMMC Assessment Scope Level 2, Version 2.0, December 2021



Steps to Scope Your Boundary



• Credit to Mark DeBry and Koren Wise





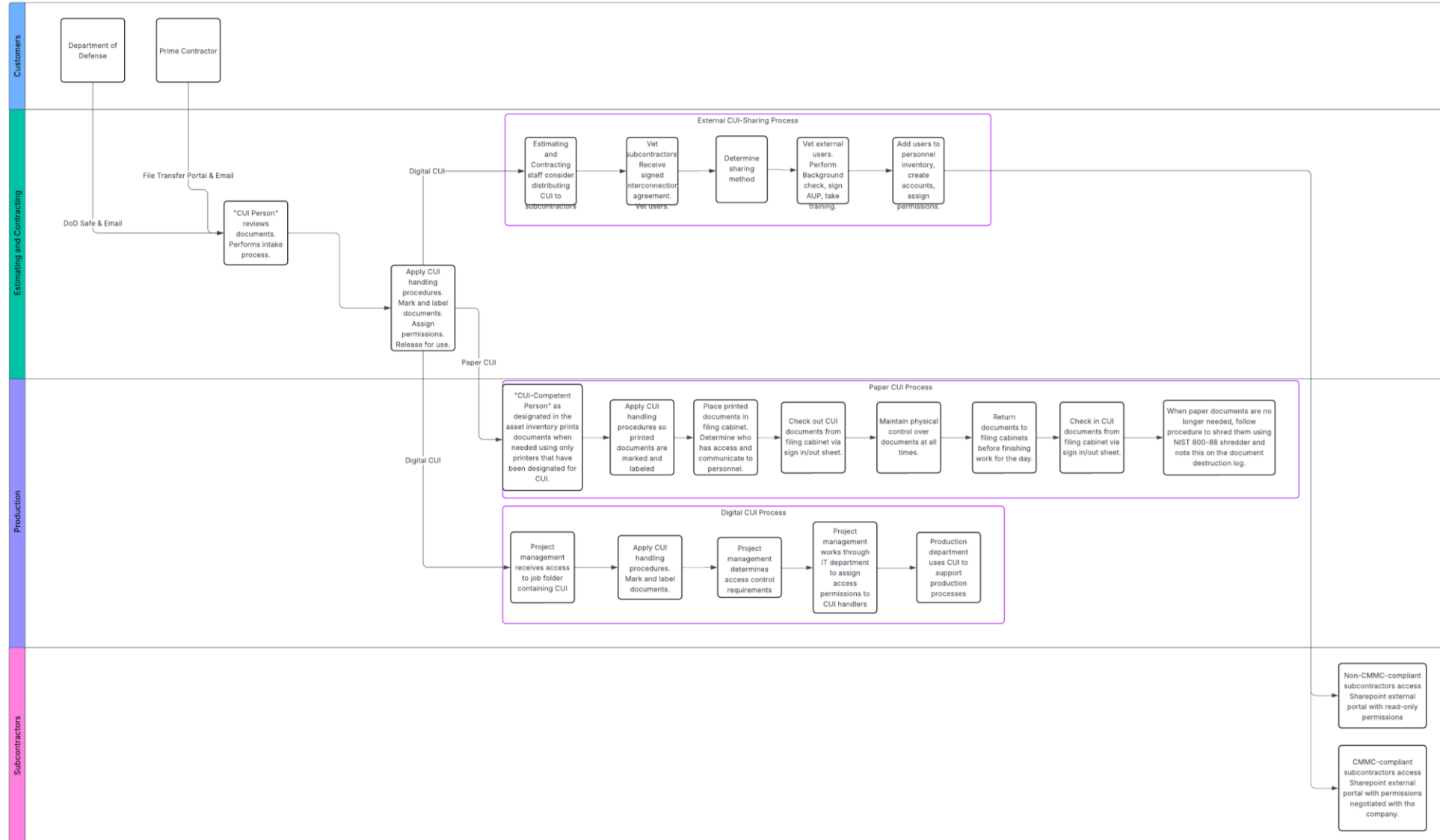
This Matters Because...

- We need to include a lot of stuff in the scope
 - All assets that store, process, or transmit CUI
 - Everything that supports these processes, i.e. security tools
- The more stuff, the more complex. Reducing can simplify compliance, but we must include everything.
- There's a lot of 'it depends' in this process. Expertise and experience is valuable to work through this.
- Scoping has to be right. Messing it up puts contracts at risk and leaves organizations vulnerable to the False Claims Act.





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* you don't know what your CUI is

Segregating controlled data to an enclave breaks business processes

Your contracting officer doesn't support it



Multinational Engineering Firm

100-person US-based company with international presence. Mix of commercial and government contracts.

DoD contracts call for protection of CUI. Company claims DoD told them to ignore CUI requirements.

CUI is intermixed with uncontrolled data. Company doesn't know what's CUI.

Business mix is 70% commercial, 30% defense.

Computing environment is very diverse.

Security Protection Assets, processes, and documentation are incomplete.

CUI is stored in a mix of FedRAMPed and non-FedRAMPed SaaS.

Considered an enclave in a separate environment because

The current computing environment requires substantial work

The IT team has limited resources

The company has a pressing need to be CMMC compliant

This was rejected because

Isolating CUI will break business processes

The company doesn't want to run 2 computing environments

But they're reconsidering now...





Manufacturing Firm

100-person company that manufactures specially designed high-speed low-drag widgets

Build to print manufacturing

Need to print Prime's drawings for work packets and create G-Code for CNC machines

The widgets and associated technical data are classified as ITAR and CUI Controlled Technical Information

Acme does 40% DoW and 60% commercial

Current practices

G-Code programs reside on engineers' laptops

No control over USB drives used to copy G-Code and take to CNC machines

Engineers log into portals and copy drawings down to a folder on the file server

Inspection reports are stored in the ERP system

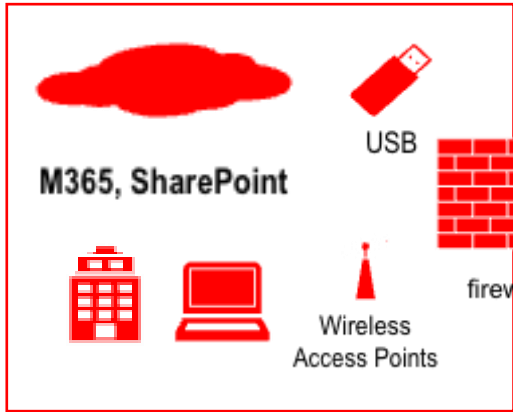




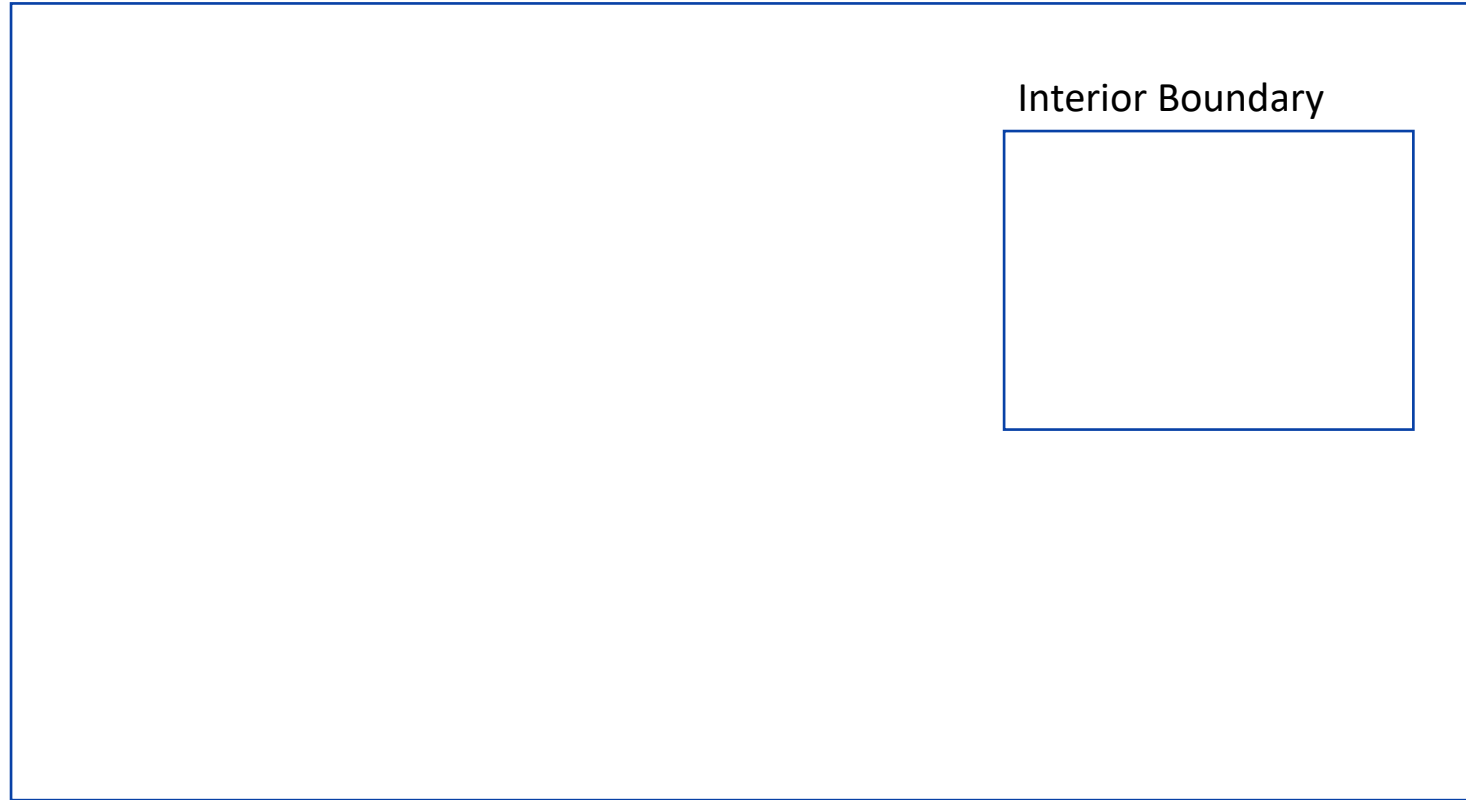
Live Scoping - Acme Manufacturing

CMMC Assessment Scope

Out of Scope



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



AVD



USB



Admin



CUI User



Printer



Machines
Specialized Asset



ERP



ERP



In scope Facilities



Fileshare



Wildcards To Watch For

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

Is your MSP or MSSP a CSP?



QUESTIONS?



Ace Swerling, Sr Compliance Consultant, CompliancyIT
aswerling@compliancyit.io
www.compliancyit.io
Tel: 724.235.8750
www.linkedin.com/aceswerling