

Cybersecurity Maturity Model Certification (CMMC) Assessment Boundary Scoping

November 9, 2022



Introduction

Carly Logan

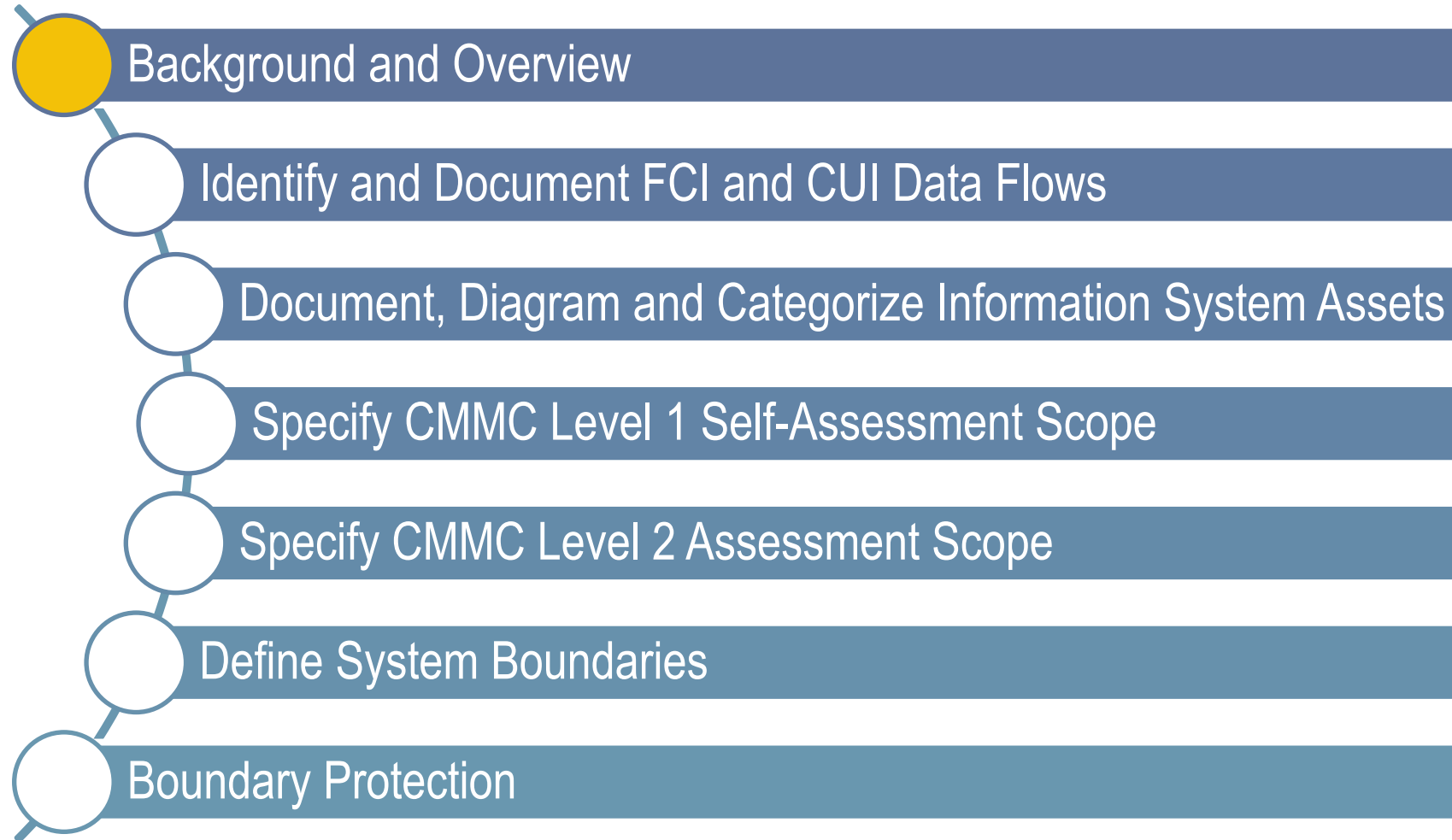
- CMMC Provisional Instructor
- CMMC Provisional Assessor
- Certified CMMC Professional
- CISSP, CCSP, CRISC
- Senior Auditor and Advisor @ Gray Analytics, Inc.

Background

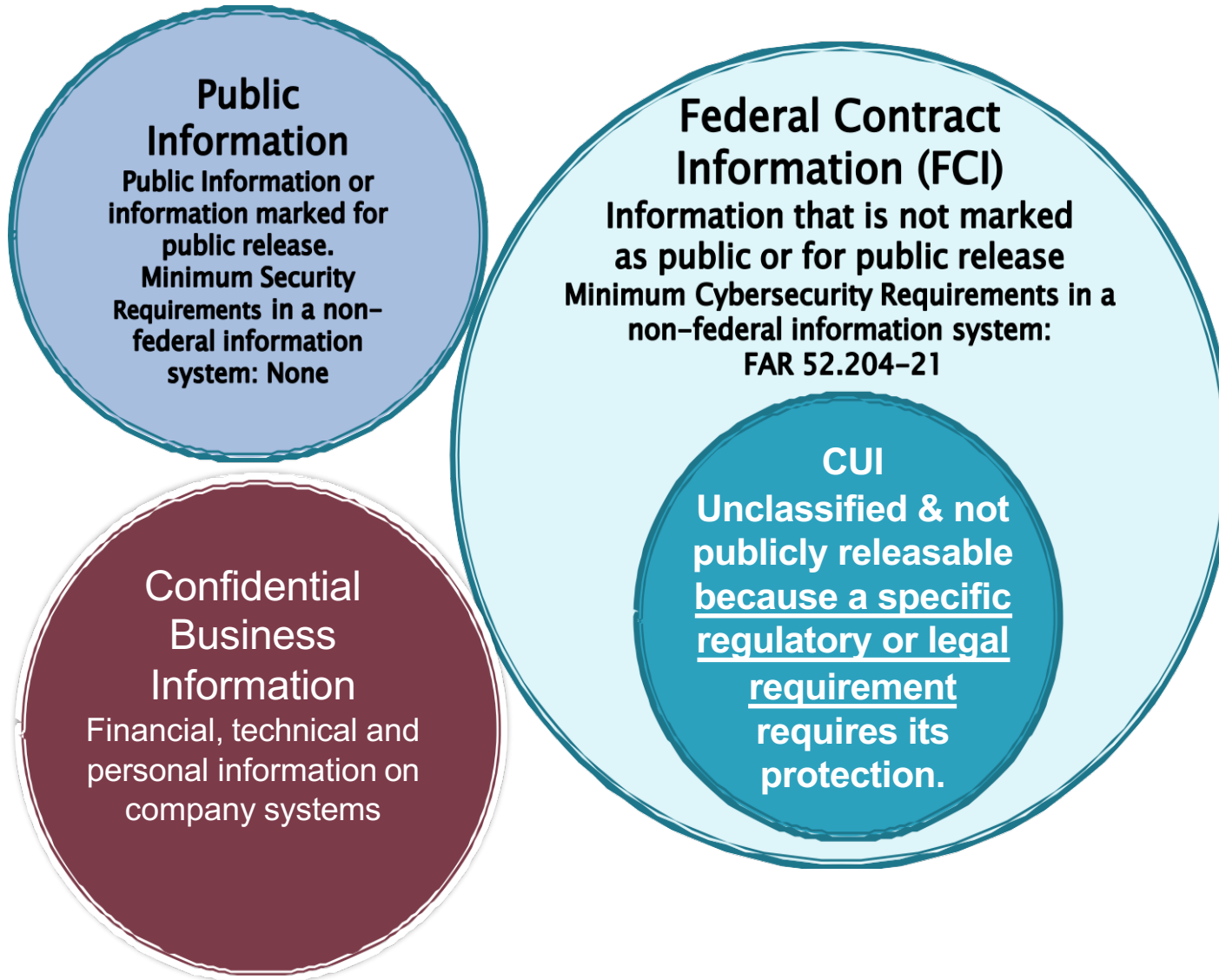
- *ORNL Cyber Risk Management & Oversight*
- *DOE Cyber-Forensics Lab (JC3) Cyber Program*
- *DOD DC3 CTA – Instructor/Researcher*

Cybersecurity Maturity Model Certification Pre-Assessment Training

CMMC 2.0 Scoping and Assessment Boundaries



Background and Overview



FCI

15 Basic FAR=
17 NIST 800-171=
CMMC Level 1

Contracts after they are issued and associated contract files

RFP responses if responses include detail that is not publicly available such as that which may be described in past performance.

CUI

DFARS 7012+
110 NIST 800-171
CMMC Level 2

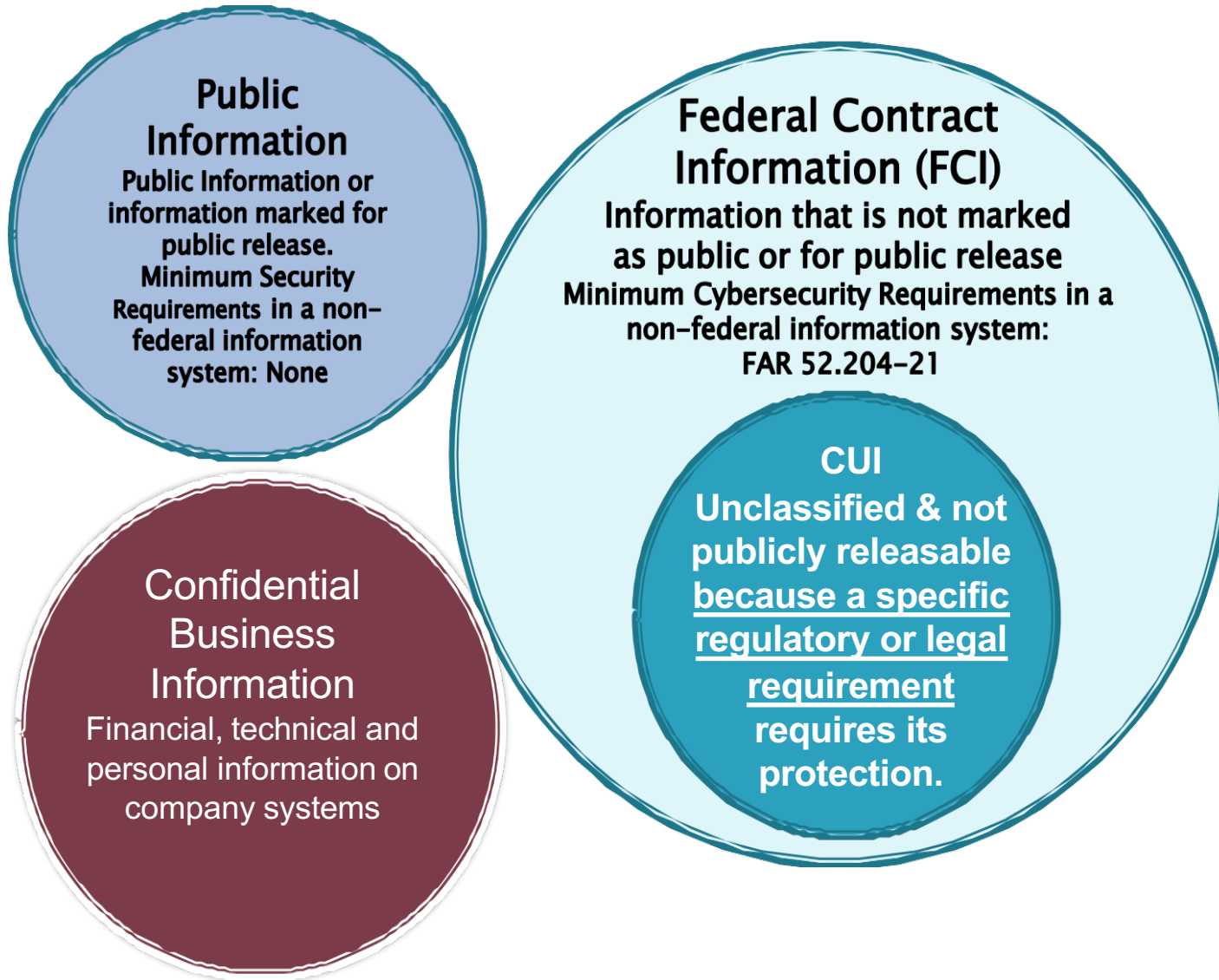
CUI Basic – CUI Specified

Controlled Defense Information (CDI)

Controlled Technical Information (CTI)

Export Controlled Data (ITAR/ECI/EAR)

Background and Overview



All CUI
is FCI
but
Not all FCI
Is CUI

Background and Overview

DFARS 252.204-7012
“Born”



Thou Shalt Protect
CUI & apply NIST
800-171

DFARS 252.204-7019
“Crawl”



Thou Shalt Enter Self-
Attestation in SPRS

DFARS 252.204-7020
“Walk”



DIBCAC: “We Shall
Trust But Verify”

DFARS 252-204.7021
“Run”

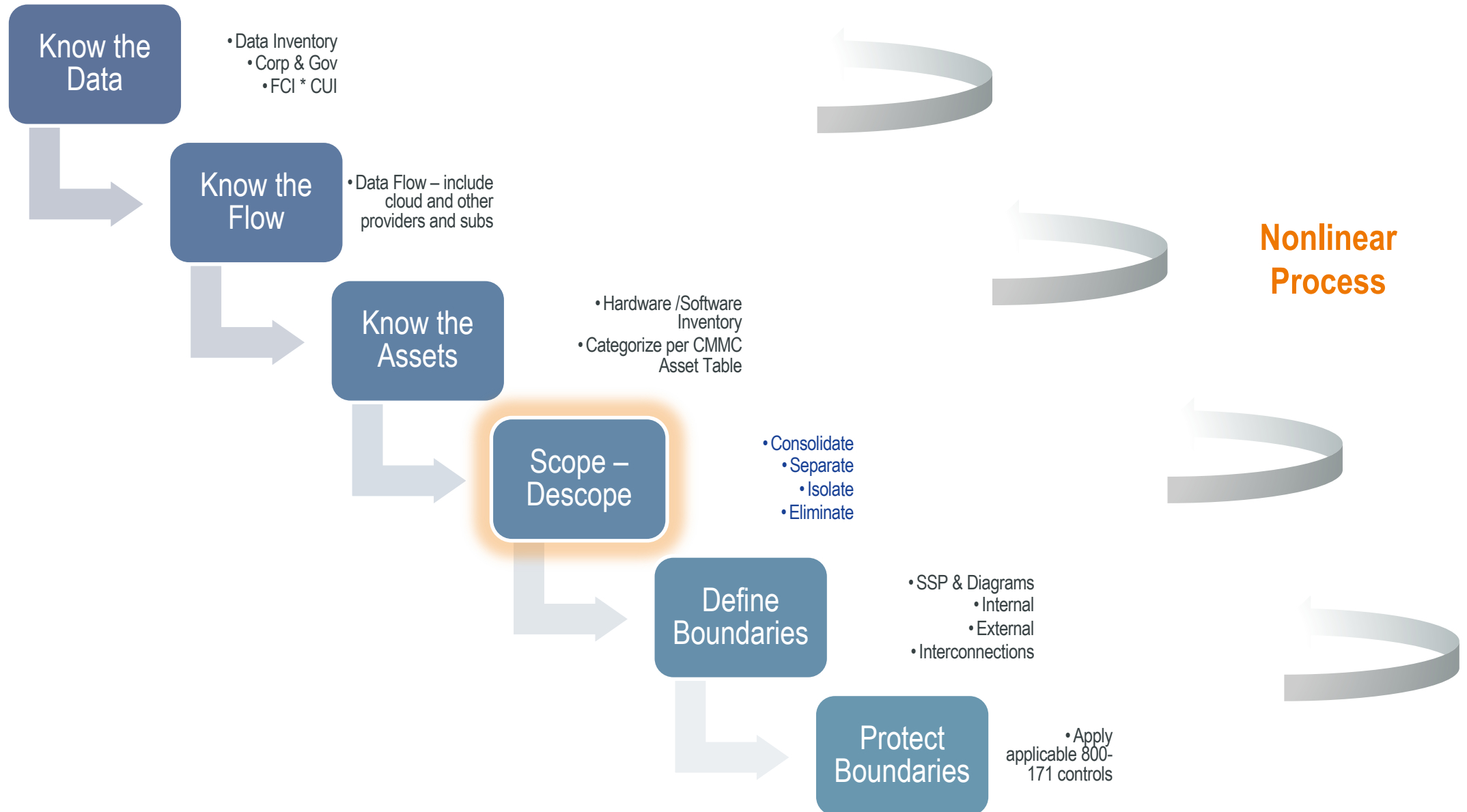


3rd Party Assessment.
Certification At Time
of Award

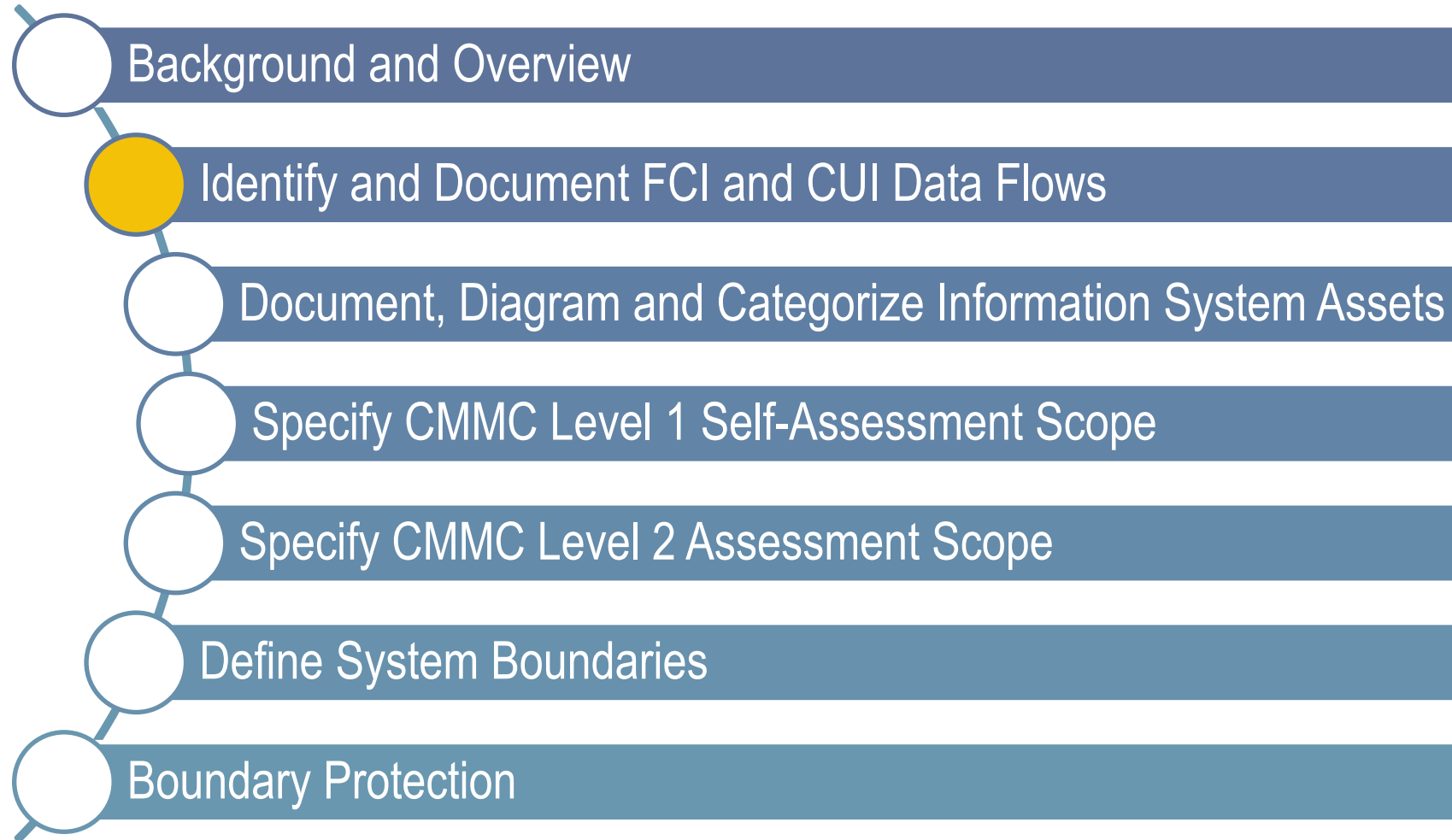
We are HERE



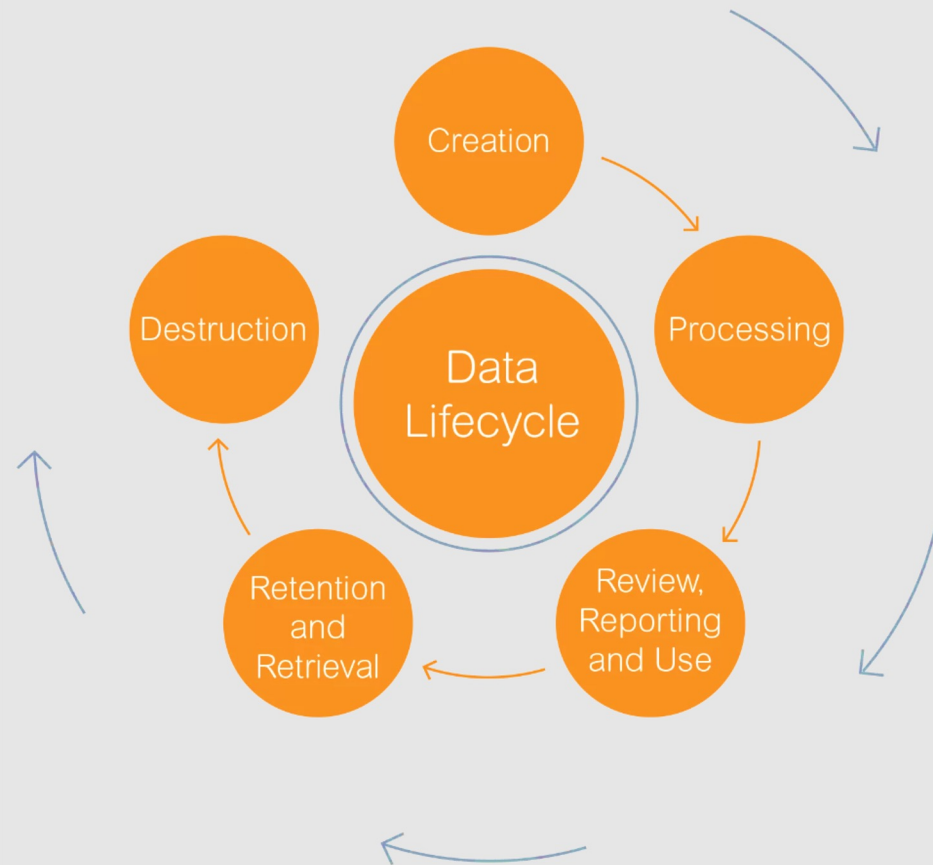
Overview – Determining What is “In Scope” for CMMC



CMMC 2.0 Scoping and Assessment Boundaries



Consider the typical data lifecycle.



Identify FCI/CUI

Identify WHO

Identify WHERE/HOW

**Consider the people,
processes and technology.**



Identify FCI/CUI

Consider the people, processes and technology in the **data** lifecycle.

Identify and inventory all federal government data the company handles or plans to handle.

- Look at existing contract language, drawings/markings, and the NARA registry.
- Is **DFARS 7012** with other CUI or Regulatory language in the contract?
- Is the data **ITAR** or **other ECI**?
- Are documents labeled **CUI** or **Controlled Unclassified Information**?
- Is information marked with “**Distribution B-F**?”
- Does data match the NARA Registry **CTI, CIS, NNPI, UCNi**?

Identify WHO Handles It

Consider the **people**, processes and technology in the data lifecycle.

Consider how, where **and by whom** data is processed, stored and transmitted & shared

- **People** - Employees, contractors, vendors, **external service provider personnel** and government customers, DoD, Primes? Subs? *Who is the data shared with?*
- **Technology** - Servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems & **who manages them**
- **Facilities** - Physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms and **who has access**
- **External Service Providers (ESP)** - External people, technology, or facilities that the organization uses, including cloud service providers, co-located data centers, hosting providers, MSPs and MSSPs.

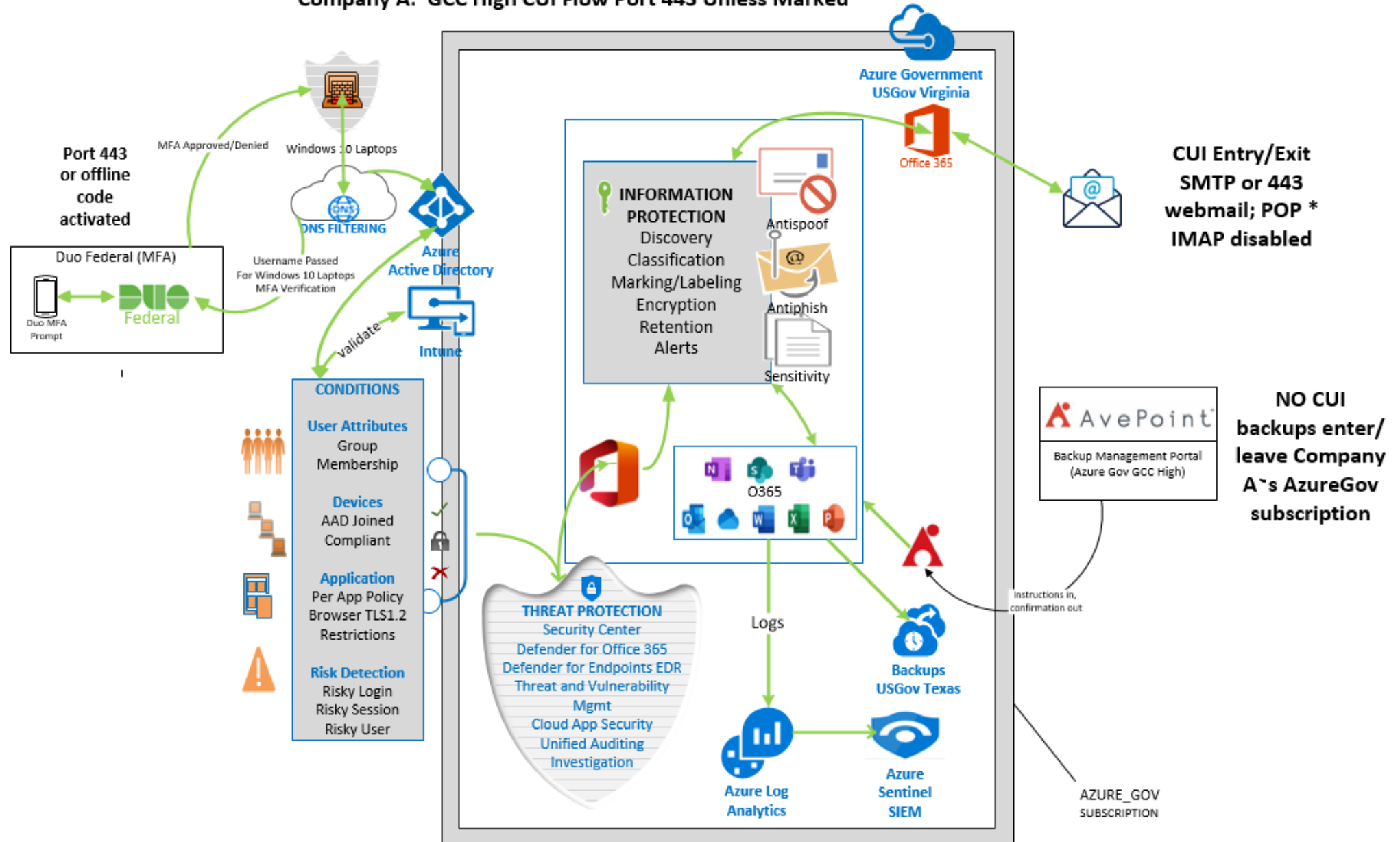
Identify WHERE/HOW What Assets

Consider the people, processes and technology in the data lifecycle.

- **Where/How:** On which user devices, over what internal network segments and devices, or across external networks, using what applications or services, websites, methods does the company receive, generate, process, share, store, transmit, archive (backup) and dispose of FCI or CUI?
 - Exostar? DoD Safe? Prime contractor drop-off? SFTP? File Shares? Email? **HardCopy?**
- **How** is FCI or CUI printed? On which printers?
- **When** is FCI or CUI stored in hardcopy/file cabinets?
- **Where** are they?
- **Where** does it go for final disposition? Shredder? Drive Destruction by IT?
- **How does Telework/Remote Offices/Alternate Sites affect the DATA FLOW?**

Sample Data Flow

Company A: GCC High CUI Flow Port 443 Unless Marked

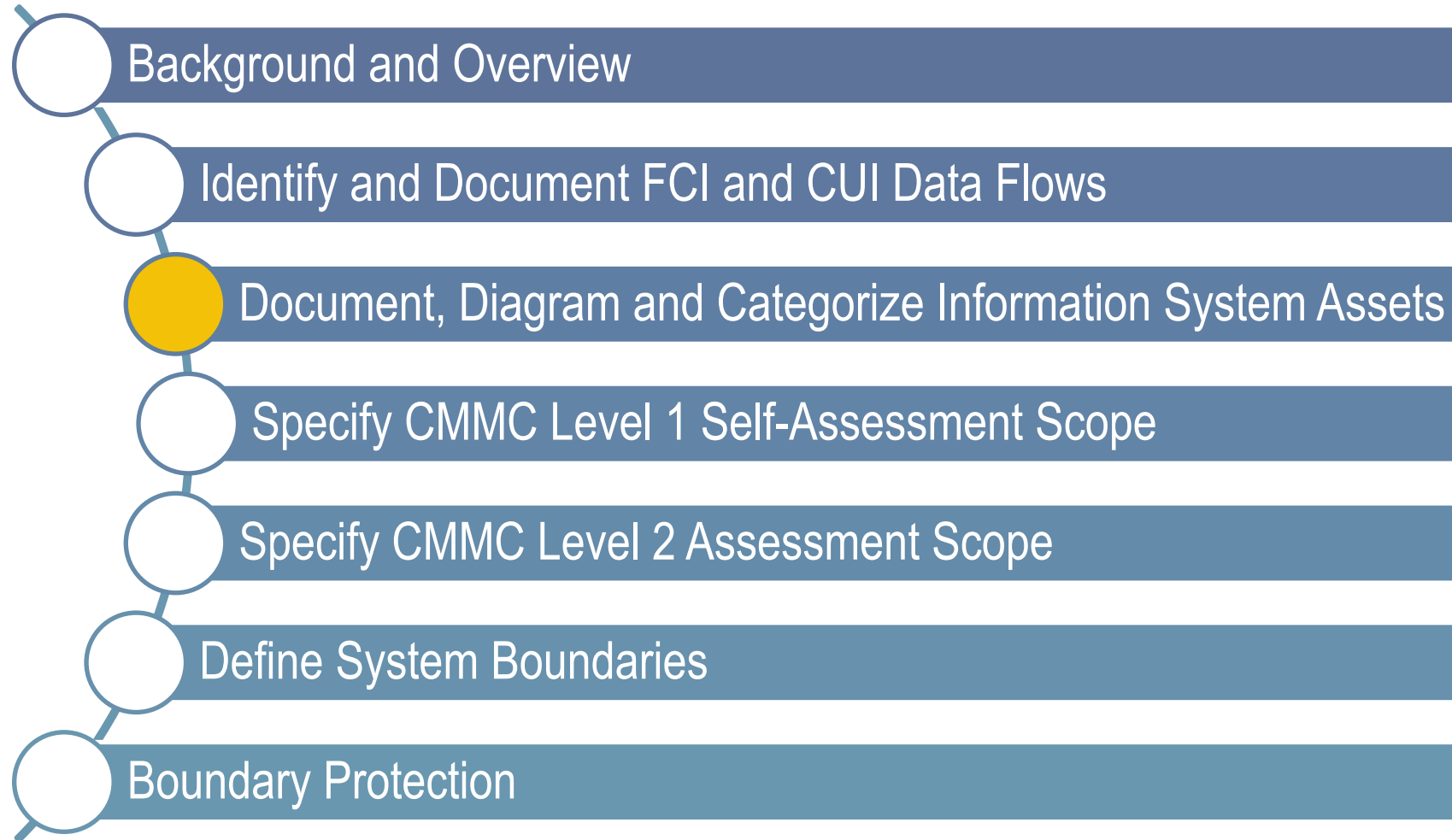


Sample Data Flow

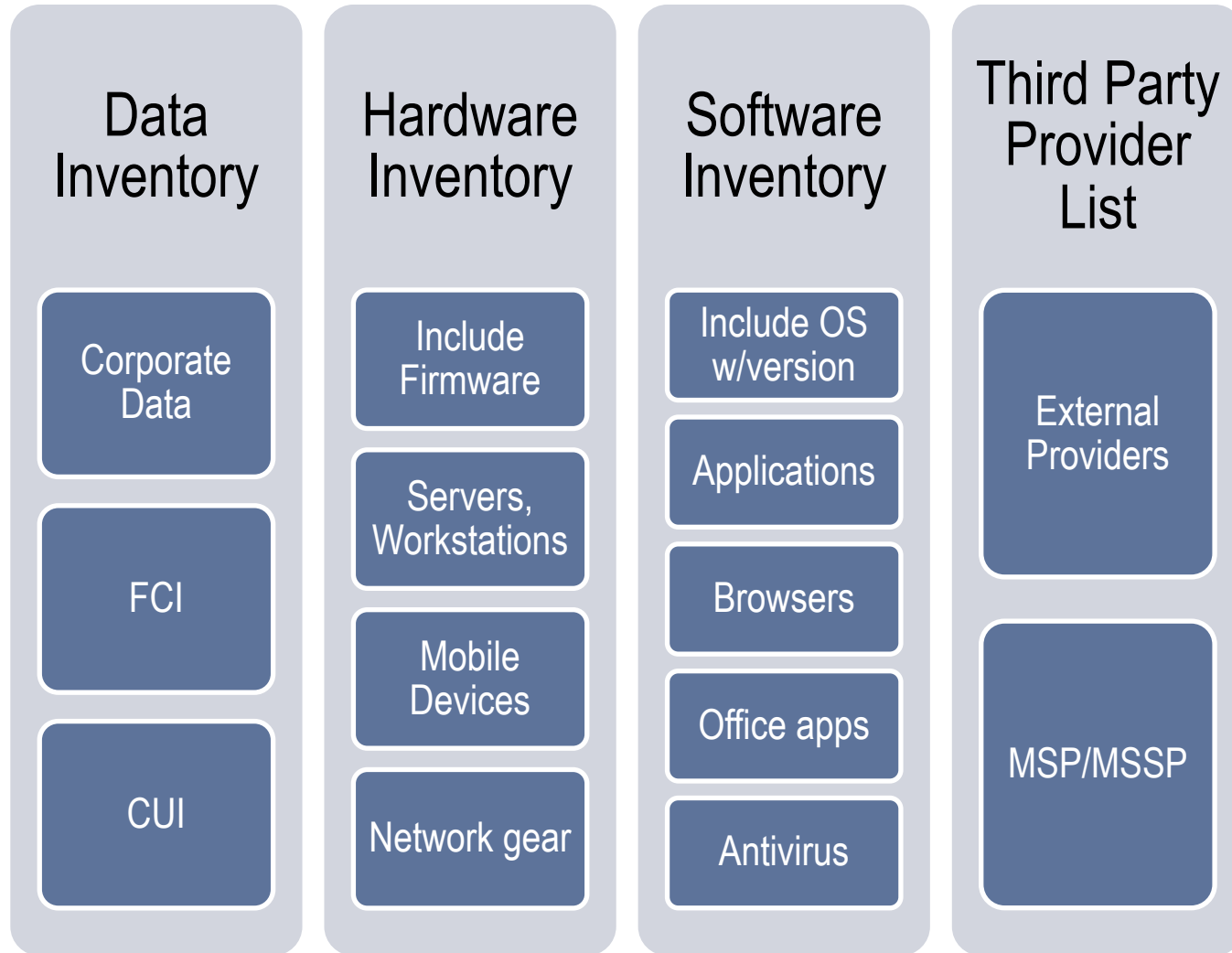
Company A: GCC High CUI Flow Port 443 Unless Marked



CMMC 2.0 Scoping and Assessment Boundaries



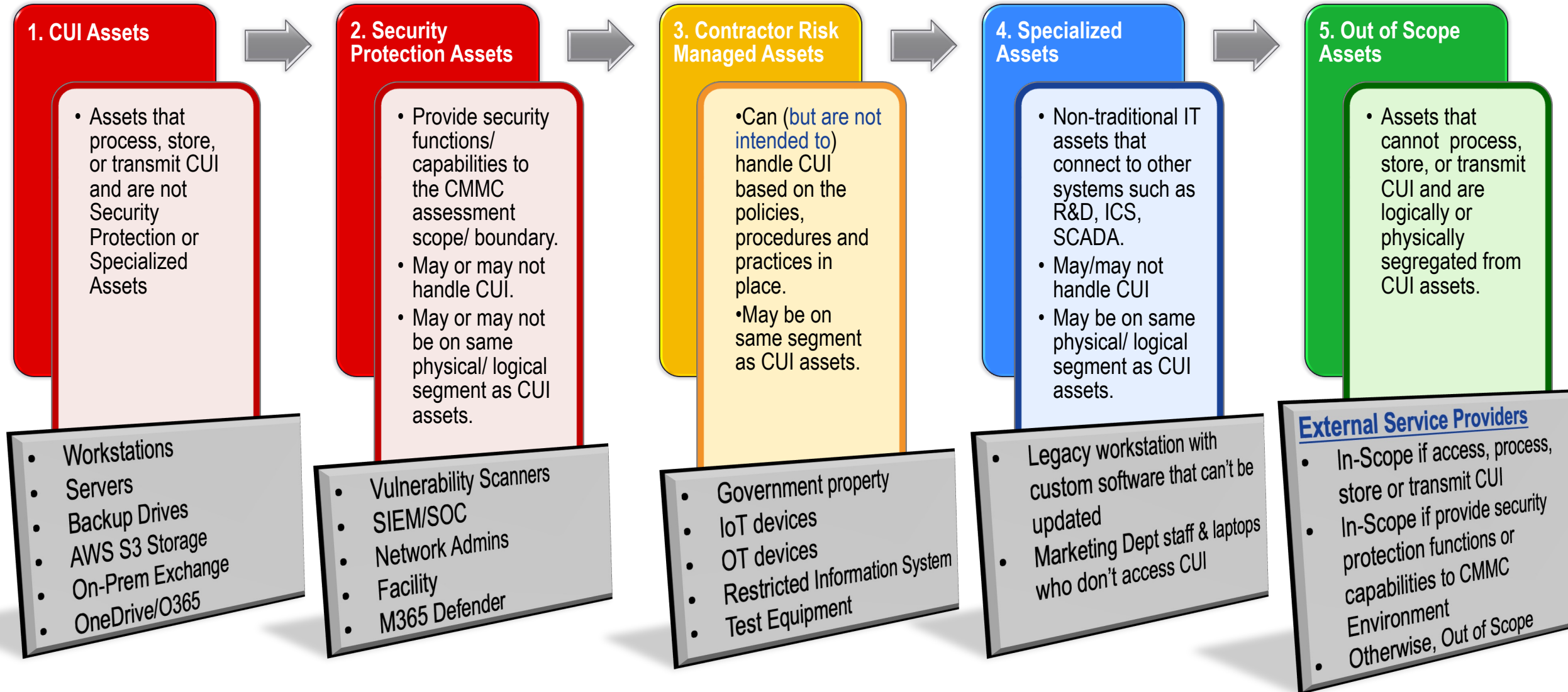
Identify and Inventory all assets.



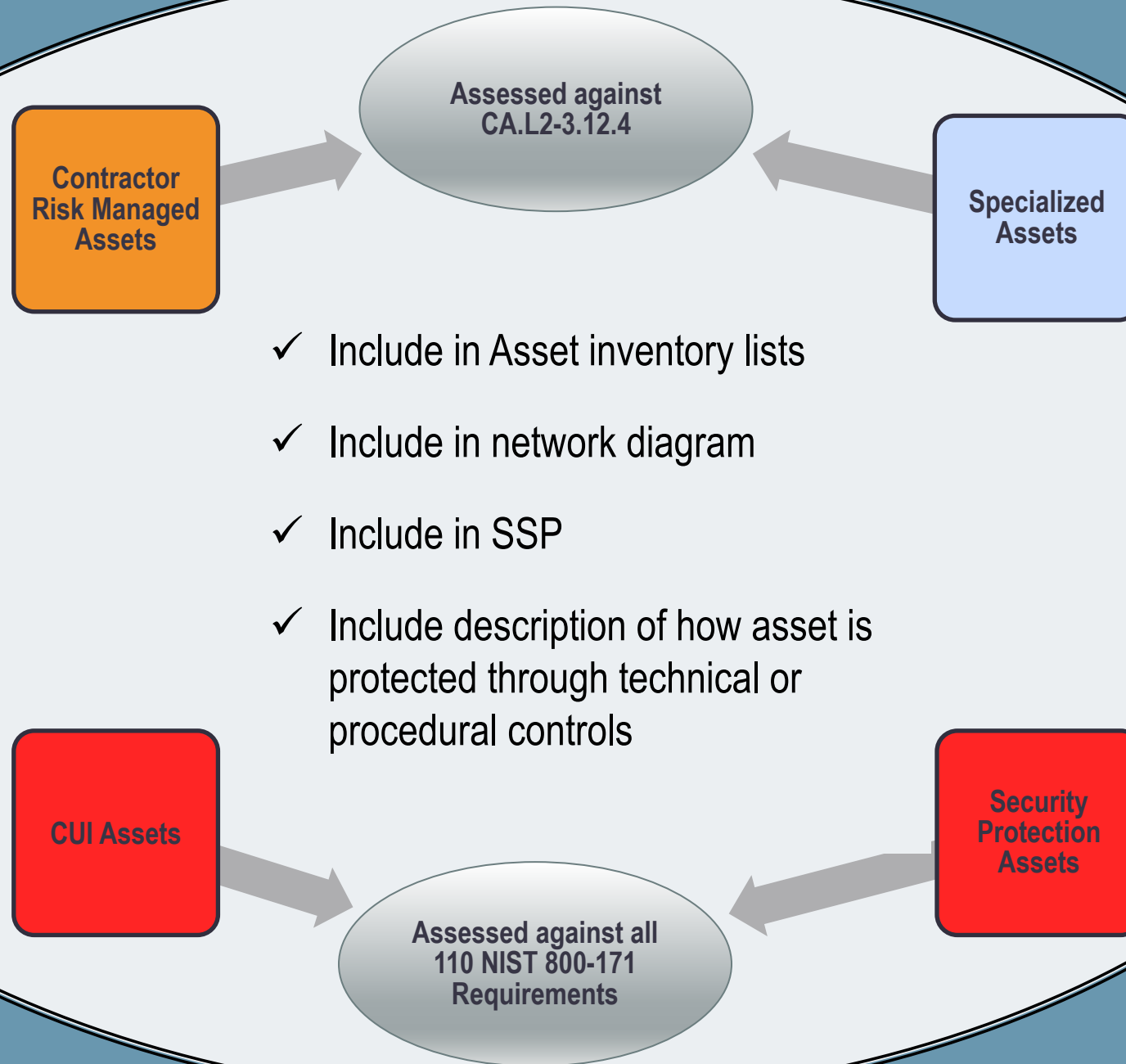
Don't forget these assets!

- ☐ All the **people** that use or access the hardware, software, and facilities
- ☐ All the physical **facilities** that house all the rest

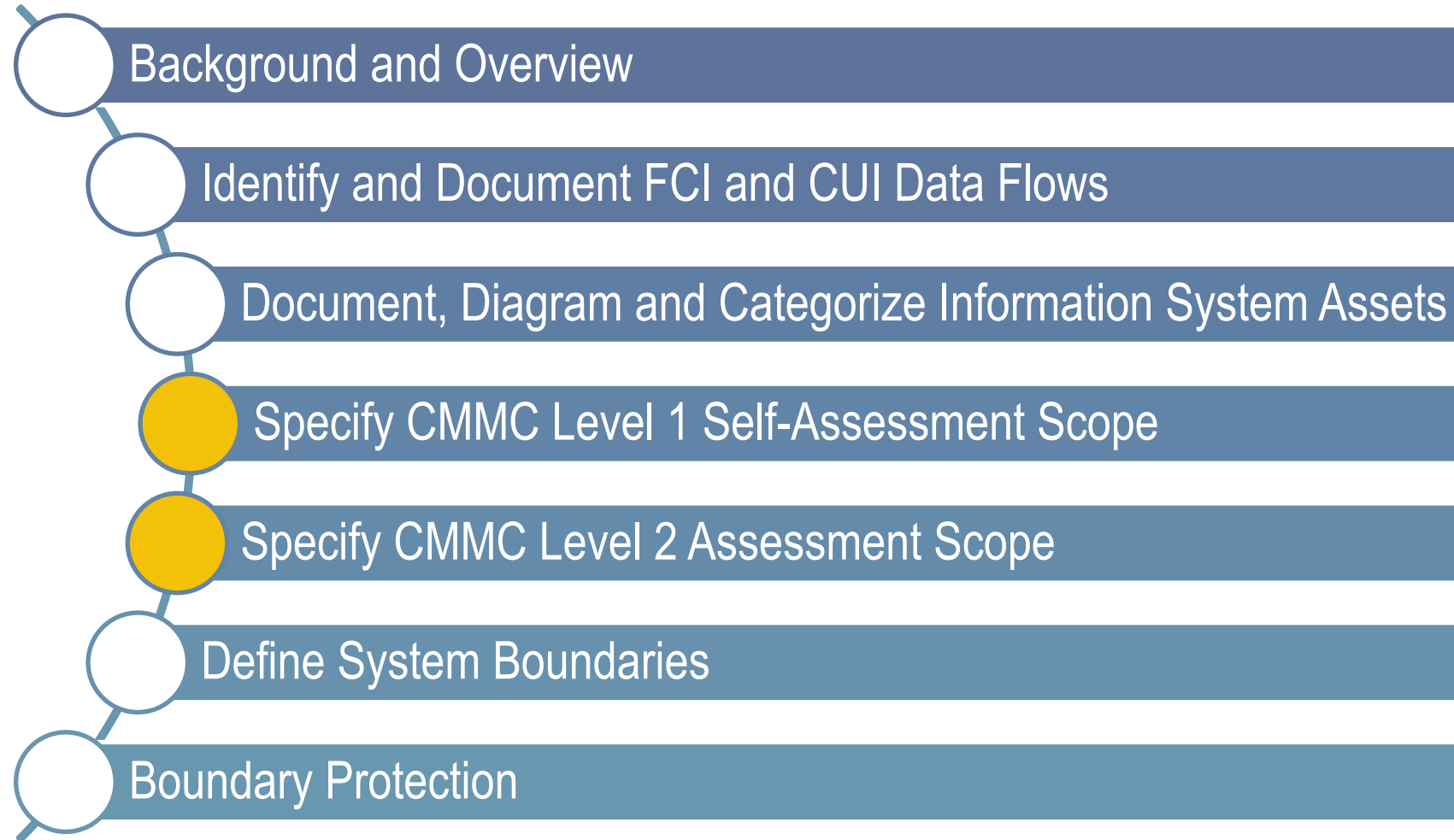
There are 5 CMMC 2.0 Asset Categories



All are In-Scope



CMMC 2.0 Scoping and Assessment Boundaries



FCI Scope CAN be Different from CUI Scope

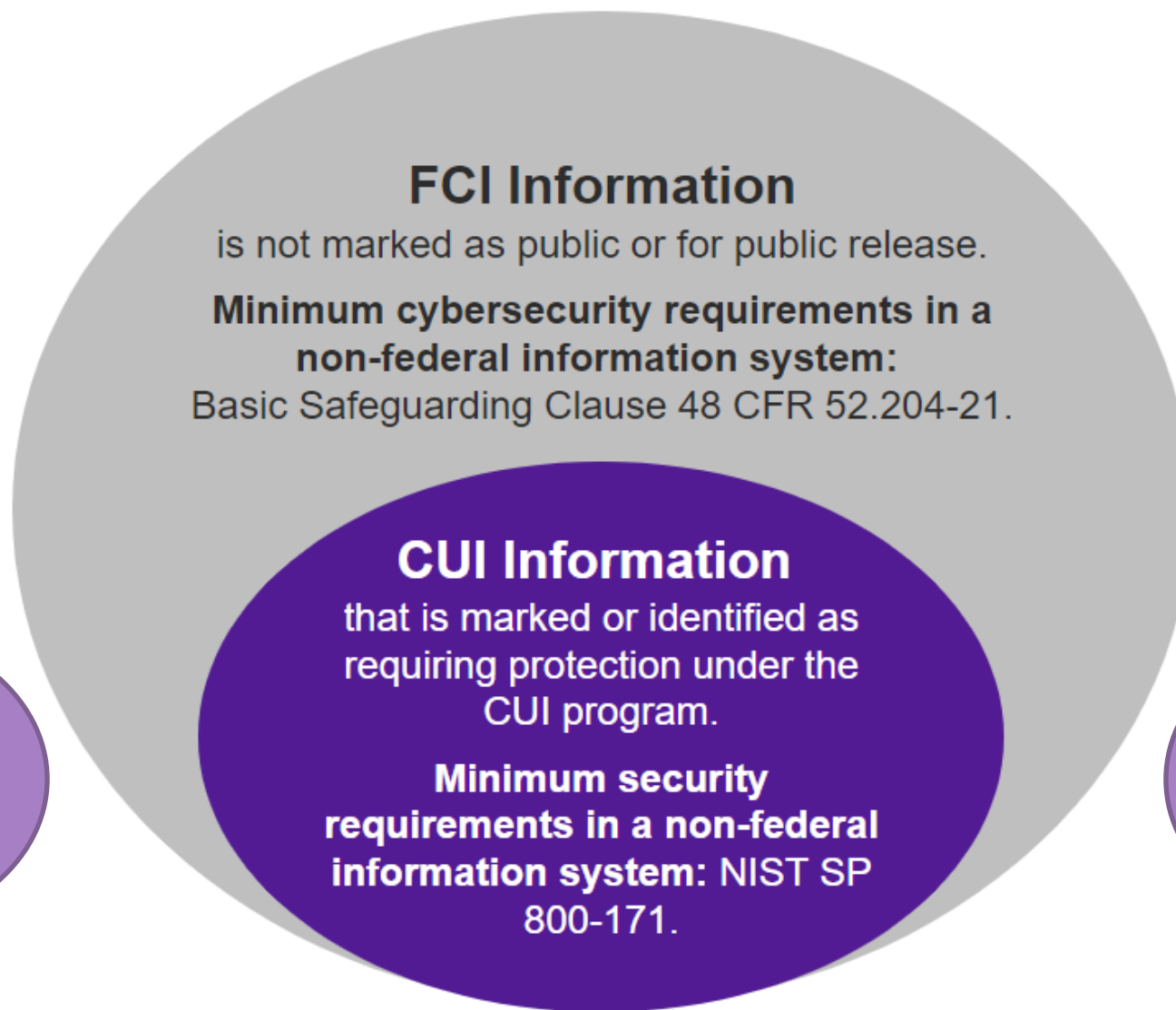
CMMC Level 1
Scope
Self-Assessment

CMMC Level 2
Scope
C3PAO

Does Enterprise or
HQ handle FCI?

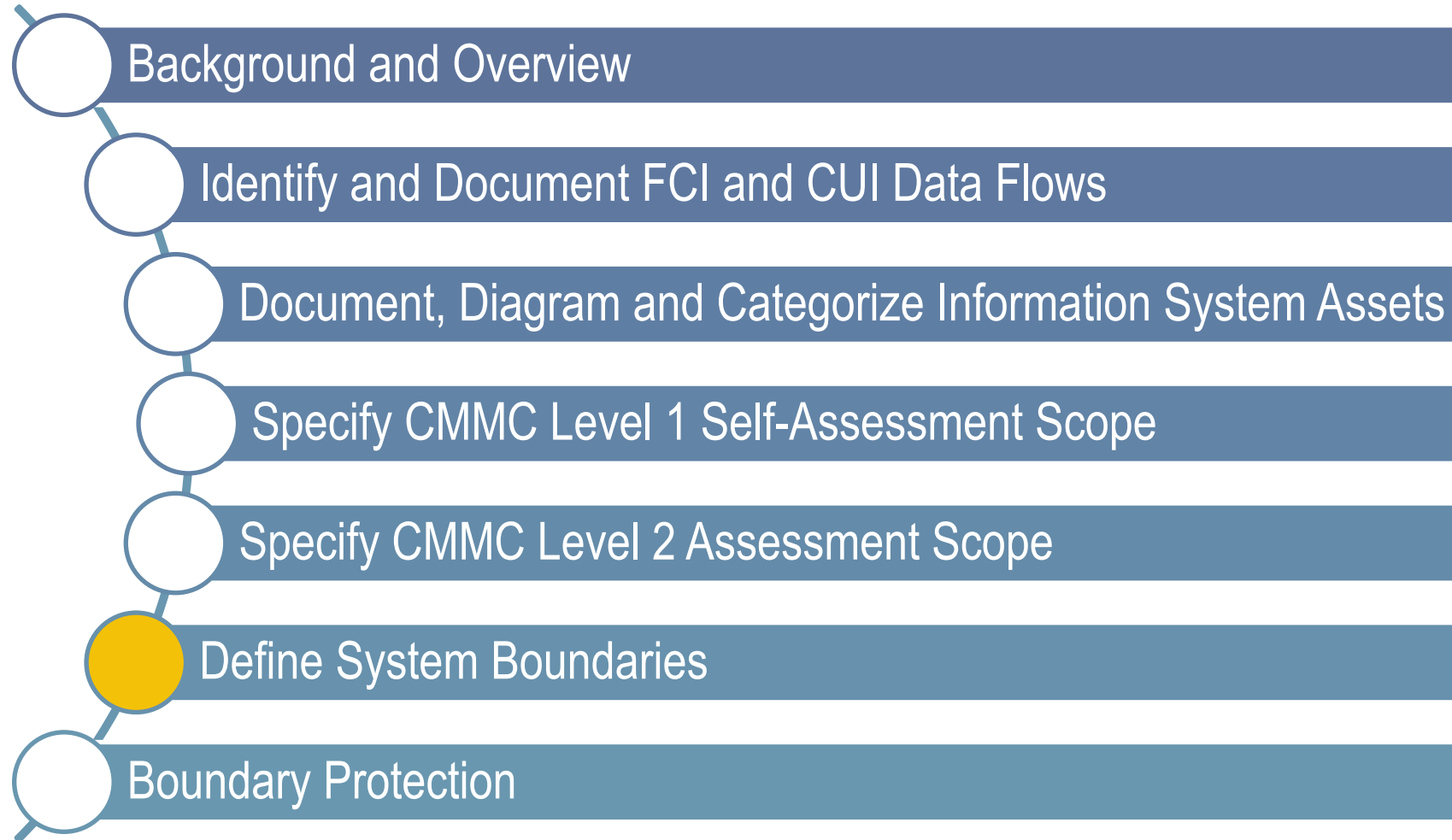
Can you “Skinny
the CUI Scope?”

CUI Zone,
Enclave,
Host Unit



CUI Zone,
Enclave,
Host Unit

CMMC 2.0 Scoping and Assessment Boundaries



What are Boundaries?

Assessment Boundary

Defines the in-scope assets and external service providers against which an assessor will evaluate conformity with applicable CMMC practices. This is the boundary for which a CMMC certificate will be applied.

An “**Information System**” in this context is the collection of assets that are combined and documented in a system security plan (SSP) that describes the assets, data flow, network, internal and external boundaries and connections to external systems outside of those boundaries. (SSP is required for CMMC Level 2 and 3)

External Information System (or component)

A system or component of a system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

May be IN SCOPE for CMMC.

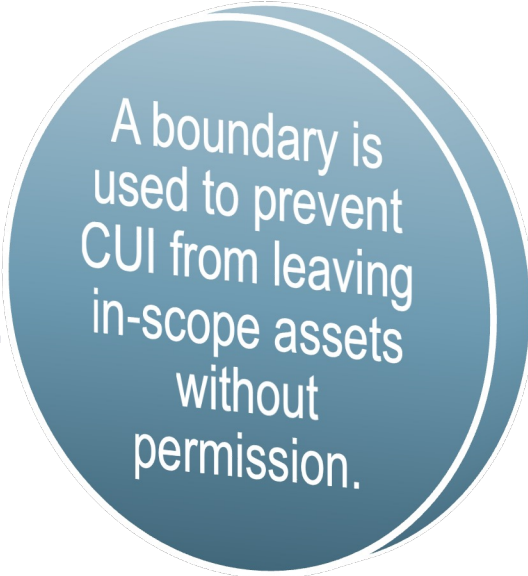
Ex: External SOC or SIEM solutions are now “Security Protection Assets” even if they do not process, store or transmit CUI. Cloud services must be FedRAMP or FedRAMP-equivalent.

Boundary & Boundary Protection

Physical or **logical** perimeter of a system.

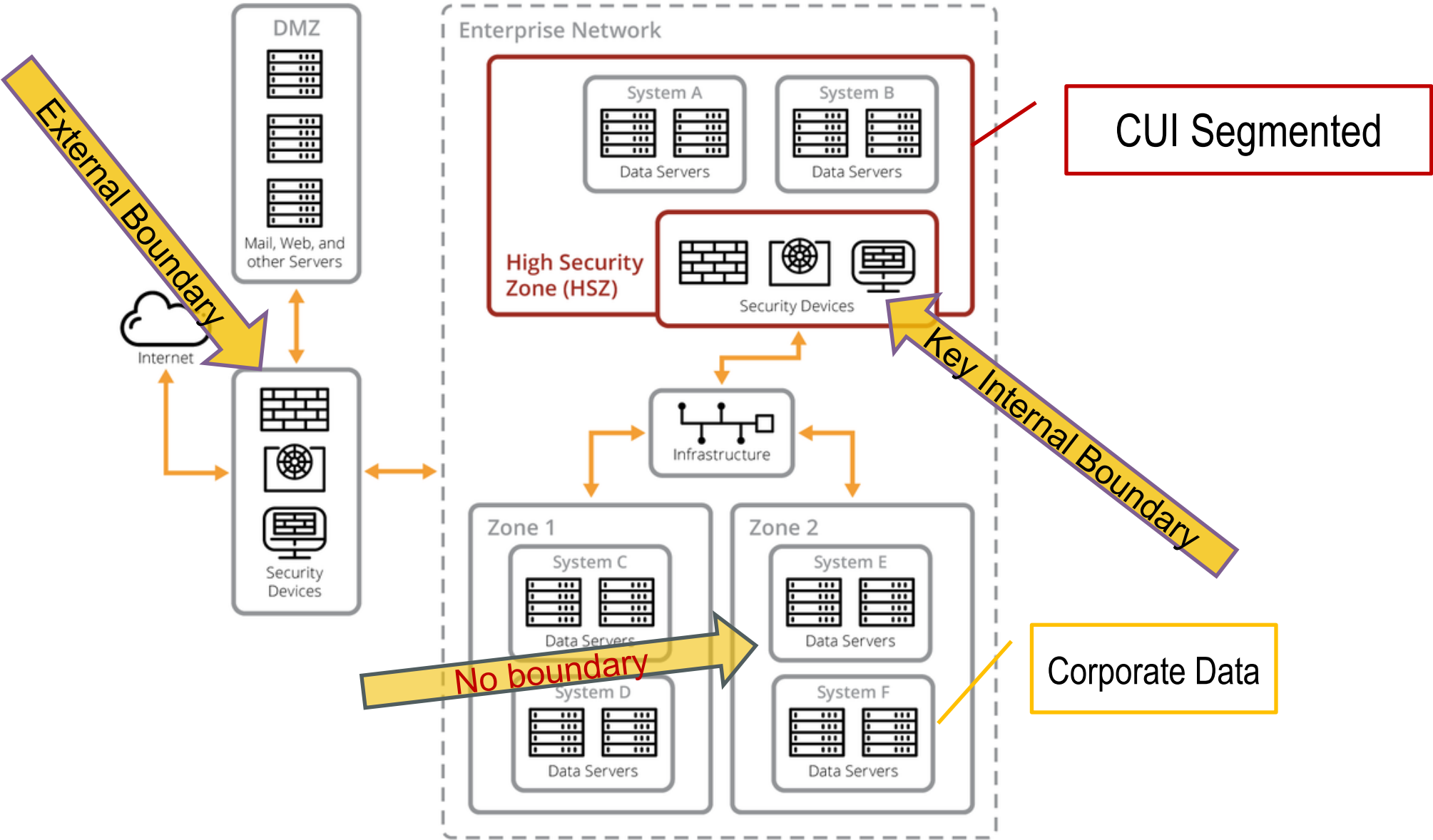
NIST 3.13.1: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the **external boundaries** and **key internal boundaries** of information systems (purpose: to prevent and detect malicious and other unauthorized communications using boundary protection devices.)

Managed interfaces include gateways, routers, firewalls, guards, network-based malicious code analysis, virtualization systems, or encrypted tunnels implemented within a security architecture.

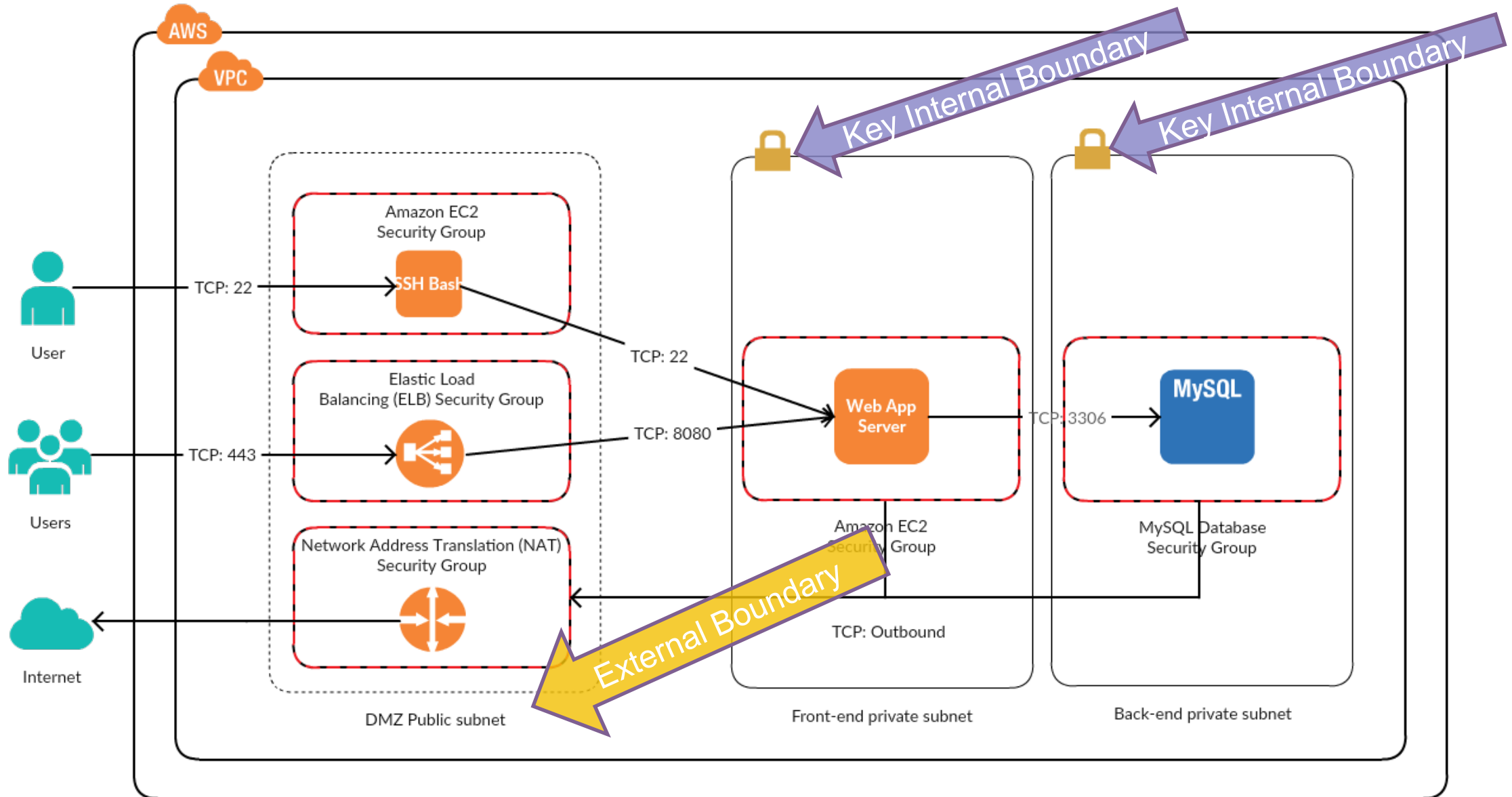


A boundary is used to prevent CUI from leaving in-scope assets without permission.

Diagram: On-Premises Internal and External Boundaries



Cloud: Internal and External Boundaries



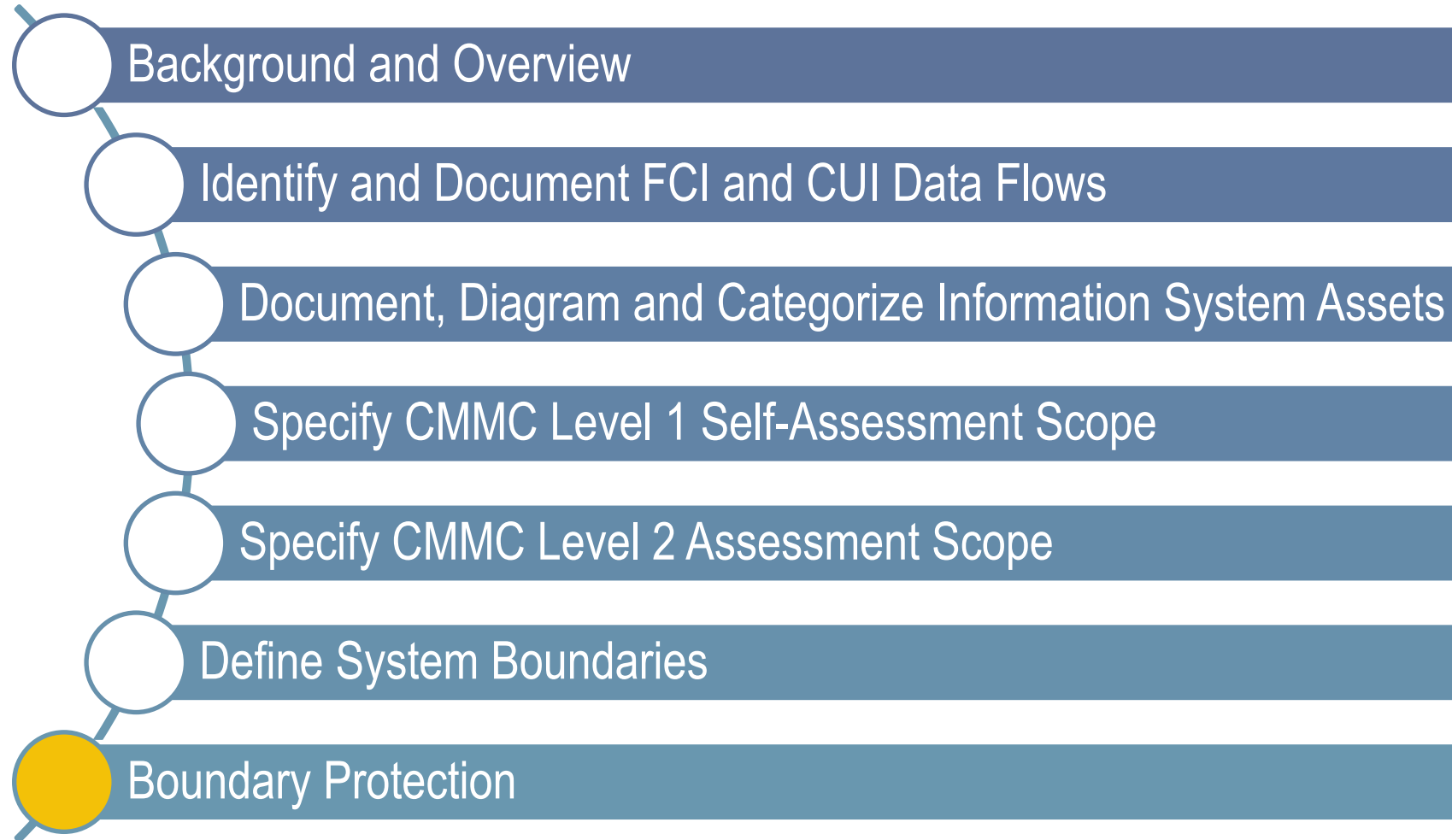
Reference: https://cdn.amazonblogs.com/security_awsblog

Assessment Scope and Assessment Boundary Recap

- ❑ We have determined what is being protected and which NIST 800-171 practices are required. (data and asset inventories)
- ❑ We have and can draw an invisible circle around all the assets, services, network segments, devices, applications, external providers, etc. that are part of the system “handling” the CUI. (assessment boundary)
- ❑ We have identified the physical and logical internal and external boundaries, be it a facility or office, borders between the Internet and the internal network, or between internal network segments.
- ❑ We have documented “interconnections” (external connections to systems outside the Assessment boundary.)
- ❑ We have updated the system description, diagrams, and mapped out the data flows.
- ❑ Important: We have also determined what the system manager does and does not have control over. And who IS responsible (i.e., another external system, cloud provider, etc.)

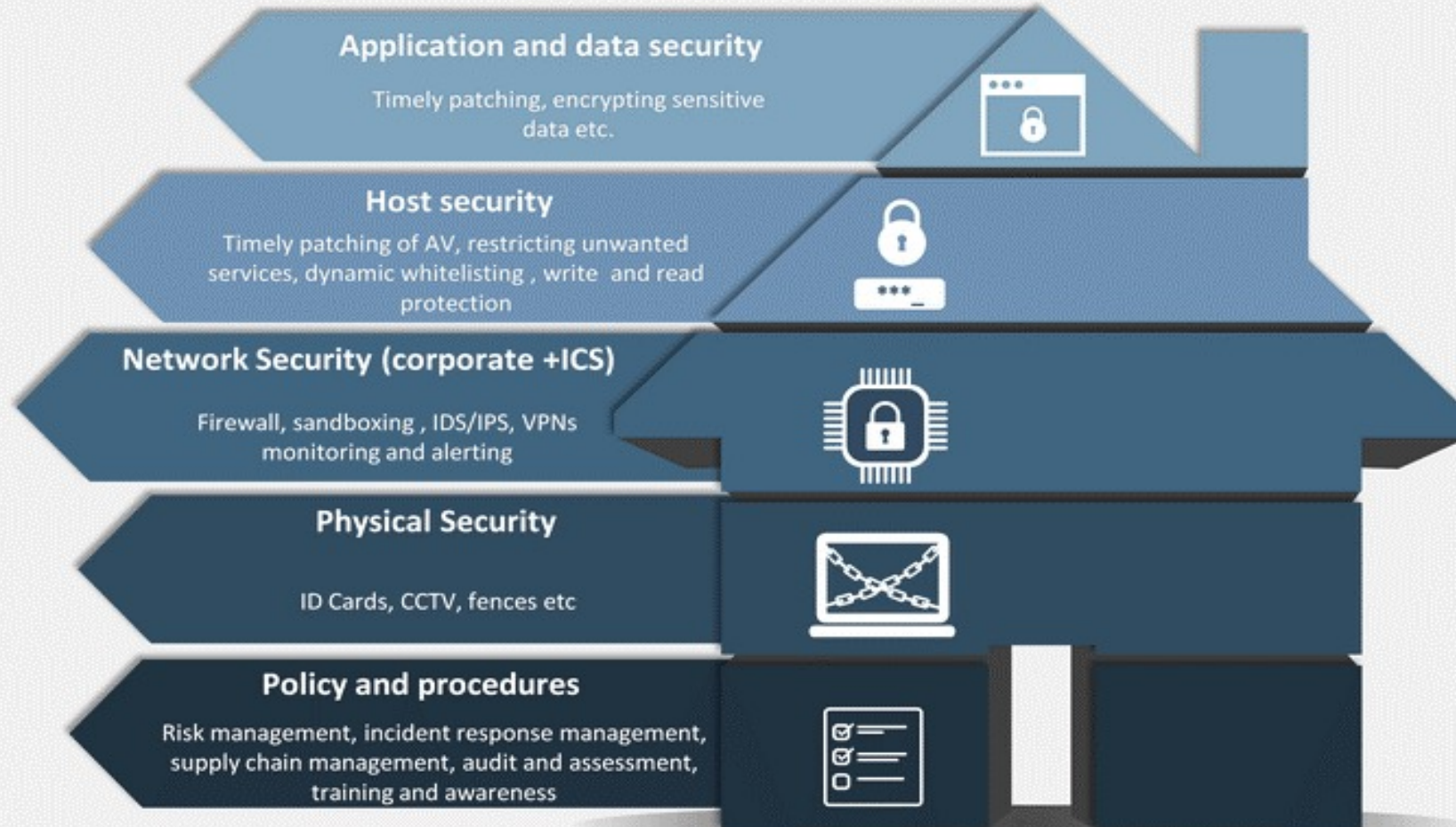
Be sure to document who is responsible for which controls in a **shared responsibility matrix**

CMMC 2.0 Scoping and Assessment Boundaries



Boundary Protection

DEFENSE IN DEPTH



Questions?

Contact:

carly.logan@grayanalytics.com

<https://www.linkedin.com/in/carlene-logan/>

