Scoping Your Organization's Security Boundary for NIST 800-171/CMMC

TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

A gap analysis can help your organization determine if you meet the requirements for achieving NIST 800-171/CMMC compliance. Establishing your organization's security boundary is a crucial early step in the gap analysis process. It's essential to accurately identify all components, systems, applications, and services that store, process, or transmit controlled unclassified information (CUI) as well as those that connect to or have the ability to connect to components that do.

Establishing Your Organization's Security Boundary

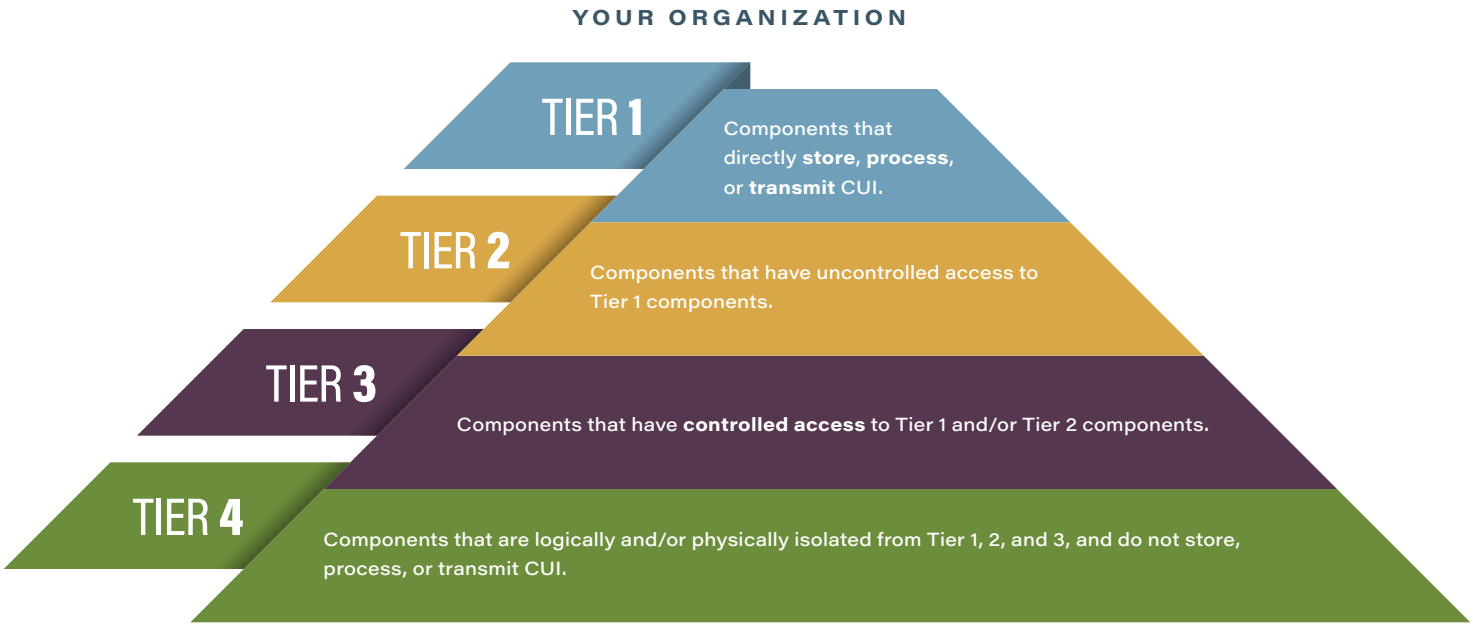
The Terrible Truth: It is shockingly easy to waste time and resources on security. That's why properly scoping your security boundary is critical to ensuring that your organization expends time and resources implementing the right requirements on the appropriate components within a well-defined boundary, not more and not less.

The term "security boundary" refers to all the system/organization components that will be considered "in scope," or subject to NIST 800-171/CMMC requirements. The term "component" refers to any part of the organization that processes, stores, or transmits CUI. Components can be both logical — hosts and network and storage devices — and nonlogical — business divisions, processes, and personnel.

If you scope too narrowly, your organization hasn't done proper due diligence to protect sensitive information. If you scope too broadly, your organization's expenditures will quickly balloon out of control, and the framework's implementation will decimate your resources. The gap analysis gives you this high-level review to help you determine the proper scoping for your enterprise.

TalaTek's Four-Tiered Approach to Properly Documenting Your Security Boundary

Tiers 1–3 are inside the security boundary and are in scope for NIST 800-171/CMMC.
Tier 4 is outside the security boundary and is not in scope for NIST 800-171/CMMC.



Controlled Access is a security technique that regulates who or what can view or use IT resources.

Scoping Your Organization's Security Boundary for NIST 800-171/CMMC

TALATEK LLC
COMPLIANCE THROUGH RISK MANAGEMENT

Using TalaTek's Four-Tiered Approach to Properly Document Your Organization's Information System

You have identified your components and sorted them by Tier. Now what? Create the System Security Plan!

Part of the gap analysis is developing your System Security Plan (SSP). The SSP is vital for your security program to be a success. Understanding your security boundary gives you the information you need to create the SSP's two major aspects:

1) **System Boundary Diagram:** This is a visual depiction of the system that the NIST 800-171/CMMC requirements are applied to. It is a logical diagram and must include all Tier 1-3 components. It should also clearly depict data ingress/egress points and any external connections made from Tier 1-3 components to external components.
2) **Requirement Implementation Statements:** For every requirement, the SSP needs to have an associated implementation statement that describes how your organization is meeting that requirement.

Two key considerations:

- **Components may have differing implementations.** Each implementation statement should address ALL component implementations. If components have differing access methods, each method should be fully documented in the associated implementation statement.
- **Organizational programs may apply across components.** Think of organization programs such as Incident Response and Configuration Management; they likely apply to all components. When documenting implementation statements, consider the applicability of the statement to all components in the boundary.

Examples of CUI

- Research and engineering data, such as drawings or formulas
- Specifications and standards
- Process sheets
- Manuals
- Technical reports

Examples of Systems, Applications, and Services

- Servers
- Workstations
- Network devices (e.g., routers, VPN)
- Mobile devices
- Removable media
- Databases
- Third-party service providers
- Cloud instances
- Major applications (including the servers and databases they depend on)

FedRAMP CERBERUS SENTINEL StateRAMP