CM.L2-3.4.6

Configuration Management

Least Functionality

"Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities."

Objectives

[a]

Essential system capabilities are defined based on the principle of least functionality.

[b]

The system is configured to provide only the defined essential capabilities.

Key Discussion Points

Defaults Are the Enemy:
Systems ship with unnecessary services, ports, and applications enabled by default — every one left running is an unneeded attack surface.

Define First:
Start by defining what the system needs to do its job — everything else is a candidate for removal or disabling.

Ports and Protocols:
Unused or unnecessary ports and protocols must be disabled — not just undocumented, actually turned off at the firewall and host level.

Ongoing, Not One-Time:
New software installs and updates can re-enable services — least functionality must be re-evaluated whenever the system changes.

Assessment Methods

EXAMINE

Configuration management policy; configuration management plan; procedures addressing least functionality; system security plan; system design documentation; system configuration settings; security configuration checklists.

INTERVIEW

Personnel with security configuration management responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes prohibiting or restricting functions, ports, protocols, or services; mechanisms implementing restrictions or prohibition of functions, ports, protocols, or services.

CM.L2-3.4.6

CONFIGURATION MANAGEMENT — Least Functionality

Plain English

What this control is really saying:

Every feature, service, port, and application that isn't needed is a door an attacker can walk through. This control requires stripping systems down to what they actually need to do their job — nothing more. If the workstation doesn't need to run a web server, turn it off. If port 23 isn't used, close it.

How it is used:

- New systems are built from a hardened image — unnecessary services are removed before deployment, not after.
- A port scan is run against all CUI systems quarterly — any open port not on the approved list triggers an immediate review.
- Group Policy disables USB storage, Bluetooth, and remote desktop on all workstations that do not require these functions.
- The file server runs only file sharing services — no web, print, or application services are installed on the same system.

Real World Example

The Scenario

Acme Defense deployed its CUI file server directly from the vendor's Windows Server image. The IT admin installed a few extra tools during setup — IIS web server, FTP service, and Telnet — because 'they might be useful later.'

What the assessor finds

IIS, FTP, and Telnet are all running and listening on the network. Port 21 and port 23 are open on the firewall. No essential capability baseline has been defined. The file server is performing three additional functions it was never authorized to perform.

SPRS Score Impact

3.4.6 carries a point value of 5. Unnecessary services are the most commonly exploited attack surface in DIB environments — attackers scan for open ports and default services because they know most organizations never turn them off.

What Good Looks Like

Essential capabilities defined per system type, systems built from hardened images with unnecessary services removed, ports and protocols restricted at host and network level, configuration verified quarterly, deviations reviewed and approved.

Common Gaps

What assessors actually find in the field:

✗ **Default install deployed as-is**

Systems are deployed straight from the vendor image with no hardening — all default services and ports remain active.

✗ **Essential capabilities undefined**

Nobody has defined what each system actually needs to do — so nothing can be meaningfully removed.

✗ **Services disabled but not documented**

Some hardening was done informally — there is no record of what is essential versus what was removed.

✗ **Unnecessary software installed**

Workstations have games, media players, and development tools that serve no business function in the CUI environment.

✗ **No ongoing verification**

Systems were hardened at build time but software updates and new installs have re-enabled services over time.