CM.L2-3.4.1

Configuration Management

System Baselining

"Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles."

Objectives

[a]
A baseline configuration is established.

[b]
The baseline configuration includes hardware, software, firmware, and documentation.

[c]
The baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.

[d]
A system inventory is established.

[e]
The system inventory includes hardware, software, firmware, and documentation.

[f]
The inventory is maintained (reviewed and updated) throughout the system development life cycle.

Key Discussion Points

Two Deliverables:
This control requires two artifacts: a baseline configuration AND a system inventory. Both must exist and be maintained.

What Goes In a Baseline:
Software versions, patch levels, config settings, network topology, and component placement — not just a list of what is installed.

What Goes In Inventory:
Hardware specs, software license info, version numbers, component owners, machine names, and network addresses for networked devices.

Living Documents:
Both the baseline and inventory must be updated when systems change — a snapshot from two years ago does not satisfy this control.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing baseline configuration; system inventory records; inventory review and update records; system architecture and configuration documentation; system configuration settings; change control records; system security plan.

INTERVIEW

Personnel with configuration management responsibilities; personnel with responsibilities for establishing and updating the system inventory; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for managing baseline configurations; mechanisms supporting configuration control; organizational processes for developing, documenting, and updating system inventory.

CM.L2-3.4.1

CONFIGURATION MANAGEMENT — System Baselining

Plain English

What this control is really saying:

You cannot secure what you have not documented. A baseline tells you what your systems are supposed to look like. An inventory tells you what you actually have. Without both — maintained and current — you cannot detect unauthorized changes, enforce security configurations, or understand your own attack surface.

How it is used:

- A configuration baseline is documented for all Windows workstations covering OS version, installed applications, patch level, and enabled services.
- The system inventory is maintained in a spreadsheet covering all hardware (make/model/serial), software (name/version/license), and firmware.
- Baseline and inventory are reviewed quarterly and updated whenever a system is added, removed, or significantly changed.
- Configuration settings are enforced via Group Policy — deviation from baseline triggers an alert and corrective action.

Real World Example

The Scenario

Acme Defense has grown from 5 to 18 workstations over three years. Systems were built as needed with no standard image. They recently hired a consultant who asked for the system inventory and baseline configuration to complete an SSP.

What the assessor finds

No baseline configuration exists. The inventory is a partial list of desktops created four years ago — it is missing five workstations, the file server, and all network devices. Software versions and firmware are not documented anywhere.

SPRS Score Impact

3.4.1 carries a point value of 5. Without a baseline and inventory, the entire CM domain collapses — you cannot detect change, enforce configuration, or assess impact without knowing what you started with.

What Good Looks Like

Documented baseline for all system types, comprehensive inventory covering hardware/software/firmware, both reviewed and updated quarterly and on system change, inventory tied to change control process.

Common Gaps

What assessors actually find in the field:

✗ **No baseline exists**

Systems were built over time with no documented baseline — nobody knows what a 'normal' configuration looks like.

✗ **No inventory**

The organization cannot produce a list of all hardware, software, and firmware in the CUI environment.

✗ **Stale baseline**

A baseline was documented two years ago but never updated — it no longer reflects the actual system configuration.

✗ **Inventory not maintained**

An inventory was created for an audit but has not been updated since — new systems and software are undocumented.

✗ **Missing firmware and docs**

The baseline covers software but not firmware versions or documentation — only partially satisfies [b] and [e].