CM.L2-3.4.2

Configuration Management

Security Configuration Enforcement

"Establish and enforce security configuration settings for information technology products employed in organizational systems."

Objectives

[a]

Security configuration settings for information technology products employed in the system are established and included in the baseline configuration.

[b]

Security configuration settings for information technology products employed in the system are enforced.

Key Discussion Points

Use a Checklist:
STIGs, CIS Benchmarks, and NIST SP 800-70 checklists are the recognized sources — don't invent settings from scratch.

Most Restrictive Wins:
Settings must reflect the most restrictive configuration that still allows the system to perform its required function.

Enforce, Not Just Set:
Settings must be technically enforced — Group Policy, MDM, or equivalent — not just documented and hoped for.

Document Deviations:
Any deviation from the baseline must be reviewed, approved, and documented — undocumented deviations are a finding.

Assessment Methods

EXAMINE

Configuration management policy; baseline configuration; procedures addressing configuration settings; configuration management plan; system security plan; security configuration checklists; evidence of approved deviations; change control records; system audit logs.

INTERVIEW

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

TEST

Organizational processes for managing configuration settings; mechanisms that implement, monitor, and/or control system configuration settings; mechanisms that identify and/or document deviations from established configuration settings.

CM.L2-3.4.2

CONFIGURATION MANAGEMENT — Security Configuration Enforcement

Plain English

What this control is really saying:

Every IT product has configuration settings that affect security — password policies, disabled services, encryption settings, firewall rules. This control requires that you identify the secure settings, document them in your baseline, and then technically enforce them so systems cannot drift from the secure state.

How it is used:

- CIS Benchmark Level 1 for Windows 10 is used as the security configuration baseline for all workstations.
- Group Policy Objects enforce password complexity, account lockout, screen lock timeout, and disabled unnecessary services across all domain-joined systems.
- The firewall is configured from a STIG — all non-required ports and protocols are disabled by default.
- Any deviation from the baseline requires a written exception approved by the security officer and documented in the change control log.

Real World Example

The Scenario

Acme Defense builds its workstations from a Windows 11 installation DVD. Each machine is configured by the IT admin from memory. No security checklist is used and no Group Policy hardening has been applied to the domain.

What the assessor finds

Workstations have unnecessary services running, Guest accounts are enabled on two machines, and password complexity is not enforced by policy. The IT admin says 'the systems are set up the way I learned to do it' — no checklist or benchmark was consulted.

SPRS Score Impact

3.4.2 carries a point value of 5. Unenforced security configurations are one of the most exploited attack surfaces in DIB environments — default settings and unnecessary services are well-documented attack vectors.

What Good Looks Like

CIS or STIG-based configuration settings documented for all system types, settings technically enforced via GPO or MDM, deviations reviewed and approved in writing, configuration compliance monitored periodically.

Common Gaps

What assessors actually find in the field:

✗ No security config settings

Systems use default manufacturer settings with no hardening applied — default accounts, unnecessary services, and open ports remain.

✗ Documented but not enforced

A configuration document exists but nothing technically enforces it — admins manually configure systems differently.

✗ No deviations documented

Several systems have settings that differ from the baseline but no exception was ever requested or documented.

✗ Default passwords in use

Network devices still use manufacturer default credentials — a basic hardening requirement never applied.

✗ No checklist used

Configuration settings were invented internally with no reference to CIS, STIG, or NIST guidance.