CM.L2-3.4.3

Configuration Management

System Change Management

"Track, review, approve or disapprove, and log changes to organizational systems."

Objectives

[a]
Changes to the system are tracked.

[b]
Changes to the system are reviewed.

[c]
Changes to the system are approved or disapproved.

[d]
Changes to the system are logged.

Key Discussion Points

All Four Steps:
Track, review, approve/disapprove, and log — all four are required. A process that only tracks without formal approval is incomplete.

Change Control Board:
A CCB or change advisory meeting with relevant stakeholders is the recognized mechanism — documented in agenda and minutes.

Before Production:
Changes must be reviewed and approved before being put into production — not retroactively documented after the fact.

Covers All Changes:
Hardware, software, firmware, configuration settings, physical environment changes, and vulnerability remediations all apply.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing system configuration change control; configuration management plan; system security plan; change control records; system audit logs; change control audit reports; agenda/minutes from configuration change control meetings.

INTERVIEW

Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar.

TEST

Organizational processes for configuration change control; mechanisms that implement configuration change control.

CM.L2-3.4.3

CONFIGURATION MANAGEMENT — System Change Management

Plain English

What this control is really saying:

Any change to a CUI system — adding software, changing a config, replacing hardware — can introduce vulnerabilities or break security controls. This control puts a gate on every change: propose it, get it reviewed, get it approved, implement it, and log it. No surprise changes to production.

How it is used:

- A monthly change control board meeting reviews all proposed changes to hardware, software, and configurations — attended by the IT admin and security officer.
- Change requests are submitted via a ticketing system that tracks status from proposal through approval to implementation and verification.
- Emergency changes require after-the-fact documentation within 24 hours and are reviewed at the next CCB meeting.
- All approved changes are logged with the date, description, approver, and implementer — the log is retained as part of the configuration management records.

Real World Example

The Scenario

Acme Defense's IT admin makes all system changes as requests come in. Last month he installed new CNC control software, updated the firewall firmware, and added a new user workstation — all without any formal process.

What the assessor finds

No change log exists. No change was reviewed or approved by anyone other than the IT admin. The security officer was unaware of the firewall firmware update. No meeting or review process has ever been held.

SPRS Score Impact

3.4.3 carries a point value of 5. Uncontrolled changes are the leading cause of unintentional security degradation — every unapproved change is a potential new vulnerability introduced without review.

What Good Looks Like

Formal change control process documented in SSP, all changes tracked in ticketing system, CCB or equivalent review and approval before production, full change log maintained, emergency change documentation procedure in place.

Common Gaps

What assessors actually find in the field:

✗ **No change control process**

Changes are made whenever the IT admin decides — no tracking, no review, no approval, no log.

✗ **Changes tracked but not approved**

A log of changes exists but nobody formally reviews or approves them before implementation.

✗ **No CCB or equivalent**

Changes are made unilaterally by IT staff with no oversight from management or security stakeholders.

✗ **Emergency changes never documented**

Out-of-band changes made during incidents are never captured — they are invisible to the change record.

✗ **Log does not include all changes**

Routine config tweaks and software installs are not logged — only major upgrades go through the process.