CM.L2-3.4.4

Configuration Management

Security Impact Analysis

"Analyze the security impact of changes prior to implementation."

Objectives

[a]
The security impact of changes to the system is analyzed prior to implementation.

Key Discussion Points

Prior to Implementation:
The key word is 'prior' — security impact analysis happens before the change goes in, not during or after.

Qualified Reviewer:
The person analyzing security impact must have the technical expertise to understand what the change does to the security posture.

Not the Requester:
The guide's example explicitly shows a subject-matter expert who did not submit the change performing the review — independence matters.

Feeds into CCB:
Security impact analysis feeds the change control process (3.4.3) — a change cannot be approved without this analysis being complete.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing security impact analysis; configuration management plan; security impact analysis documentation; system security plan; analysis tools and associated outputs; change control records; system audit logs.

INTERVIEW

Personnel with responsibility for conducting security impact analysis; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for security impact analysis.

CM.L2-3.4.4

CONFIGURATION MANAGEMENT — Security Impact Analysis

Plain English

What this control is really saying:

Before any change goes into your CUI environment, someone with security expertise needs to ask: could this break something? Could it introduce a vulnerability? Could it conflict with an existing control? This is the security checkpoint that lives inside your change management process.

How it is used:

- Every change request includes a security impact section — the IT admin and security officer jointly review it before CCB submission.
- The security impact analysis reviews how the change affects existing controls, what new risks it introduces, and whether additional controls are needed.
- A new software deployment was analyzed before approval — the analysis identified it required an open port that conflicted with the firewall baseline, leading to a design change.
- Security impact analysis documentation is retained with the change control record as evidence for each approved change.

Real World Example

The Scenario

Acme Defense recently deployed a new remote monitoring tool for the CNC machines. The change went through their CCB and was approved, but no security impact analysis was performed — the CCB just reviewed functional requirements.

What the assessor finds

The remote monitoring tool opened two new inbound firewall ports and installed an agent running as SYSTEM with no least-privilege controls. Nobody analyzed these security implications before deployment. The change control record has no security analysis documentation.

SPRS Score Impact

3.4.4 carries a point value of 3. Changes that bypass security impact analysis are how organizations unknowingly degrade their own security posture — new vulnerabilities introduced by routine maintenance are entirely preventable.

What Good Looks Like

Security impact analysis required for all changes, performed by qualified personnel independent of the requester, documented in change record, findings drive control adjustments before approval, analysis retained as evidence.

Common Gaps

What assessors actually find in the field:

✗ No security analysis performed

Changes go through change control but nobody specifically evaluates security impact before approval.

✗ Requester reviews their own change

The person submitting the change also performs the security analysis — no independent review.

✗ Generic checklist only

A checkbox 'security reviewed' exists in the change form but no actual analysis documentation is produced.

✗ Post-implementation review

Security impact is reviewed after the change is deployed — finding issues at that point is often too late to reverse.

✗ No qualified reviewer

The person performing the security analysis lacks the technical expertise to evaluate the actual security ramifications.