CA.L2-3.12.1

Security Assessment

Security Control Assessment

"Periodically assess the security controls in organizational systems to determine if the controls are effective in their application."

Objectives

[a]

The frequency of security control assessments is defined.

[b]

Security controls are assessed with the defined frequency to determine if the controls are effective in their application.

Key Discussion Points

Defined Frequency:
The assessment schedule must be specified — 'periodically' is not enough. Annual is standard for DIB; the frequency must be documented in the SSP.

Effectiveness, Not Existence:
The question is not whether a control exists but whether it works — a configured control that doesn't operate as intended is a failed control.

Evidence-Based:
An effective assessment gathers evidence for each control — screenshots, logs, configuration exports, and interviews rather than just reviewing the SSP.

Feeds the POAM:
Controls found ineffective should be tracked in the POAM with corrective action plans — the assessment output drives the remediation process.

Assessment Methods

EXAMINE

Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; security assessment reports.

INTERVIEW

Personnel with security assessment responsibilities; personnel with information security responsibilities.

TEST

Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting.

Plain English

What this control is really saying:

Implementing a security control is not the same as having a working security control. This control requires periodic testing and review to verify that the safeguards documented in your SSP are actually in place, configured correctly, and producing the intended protection — not just on paper, but in practice.

How it is used:

- An annual security control assessment reviews each control in the SSP — documented evidence is gathered for each control and compared against the stated implementation.
- The assessment produces a written report identifying controls that are fully effective, partially effective, or not effective — results feed the POAM and SSP updates.
- Assessment findings are reviewed by the system owner and IT admin — controls found to be ineffective trigger corrective action with documented timelines.
- The SSP documents the assessment frequency, methodology, and the date of the last completed assessment — assessor independence is noted where applicable.

CA.L2-3.12.1

SECURITY ASSESSMENT — Security Control Assessment

Real World Example

The Scenario

Acme Defense's SSP documents 45 security controls. The SSP was last updated two years ago. No formal security control assessment has ever been conducted — the IT admin assumes the controls work because nothing obvious has gone wrong.

What the assessor finds

An assessor conducts spot checks of five controls. Two controls listed as 'implemented' in the SSP are not in place — MFA for privileged users was never configured and audit logs are not being reviewed. The SSP described what was planned, not what was built.

SPRS Score Impact

3.12.1 carries a point value of 3. A security program that has never been assessed may look complete on paper but be completely ineffective in practice — control assessment is the mechanism that closes the gap between documented and implemented.

What Good Looks Like

Assessment frequency defined in SSP, formal assessment conducted on schedule, each control tested with evidence gathered, assessment report documents results, ineffective controls tracked in POAM and corrected, results reviewed by management.

Common Gaps

What assessors actually find in the field:

✗ No control assessment conducted

Security controls are documented in the SSP but have never been assessed to verify they actually work as described.

✗ Frequency not defined

The organization plans to assess 'occasionally' but no specific frequency is defined — no schedule exists and assessments are ad hoc.

✗ Assessment lacks evidence

A 'review' was conducted but only involved reading the SSP — no testing, no evidence gathering, no verification of actual control operation.

✗ Results not documented

Control effectiveness discussions happen in team meetings but no assessment report exists to demonstrate the review occurred.

✗ Findings not acted on

A prior assessment identified three ineffective controls — none have been corrected and the findings are not in the POAM.