CA.L2-3.12.3

Security Assessment

Security Control Monitoring

"Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls."

Objectives

[a]
Security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Key Discussion Points

Not Periodic:
Monitoring must be more frequent than the periodic assessments of 3.12.1 — 'ongoing' implies a cadence driven by risk, not just annual review.

Automation:
SIEM tools, log monitors, and automated scanners provide continuous visibility that manual processes cannot — they are the practical path to ongoing monitoring.

Risk-Based:
High-risk controls warrant more frequent monitoring than low-risk ones — the monitoring plan should reflect the relative criticality of each control.

Informs Management:
Monitoring outputs — reports and dashboards — give management what they need to make timely, risk-based decisions about the security posture.

Assessment Methods

EXAMINE

Security planning policy; organizational procedures addressing system security plan development; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates.

INTERVIEW

Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan.

CA.L2-3.12.3

SECURITY ASSESSMENT — Security Control Monitoring

Plain English

What this control is really saying:

A periodic assessment (3.12.1) tells you if your controls work at a point in time. This control requires ongoing monitoring between those assessments — so that if a control degrades, fails, or a new threat emerges, you know about it in time to respond rather than discovering it at the next scheduled review.

How it is used:

- A continuous monitoring plan assigns monitoring activities to each security control — high-risk controls are monitored more frequently than low-risk controls.
- Automated tools (SIEM, vulnerability scanners, log analyzers) provide ongoing visibility into control effectiveness between formal assessments.
- Monthly monitoring reports are generated and reviewed by the IT admin and presented to management quarterly — risk-based decisions are documented.
- The SSP documents the continuous monitoring strategy including which controls are monitored, how often, by whom, and how results are reported.

Real World Example

The Scenario

Acme Defense conducts an annual security control assessment. Between assessments, no monitoring activities occur. The IT admin addresses issues reactively as they come to his attention but has no systematic process for ongoing control monitoring.

What the assessor finds

A configuration change made four months ago inadvertently disabled audit logging on the CUI file server. No monitoring detected the failure. The assessor discovers it during log review — four months of audit data are missing with no way to recover the gap.

SPRS Score Impact

3.12.3 carries a point value of 3. Organizations that rely solely on periodic assessments have significant blind spots — ongoing monitoring is the mechanism that maintains security posture between those assessments.

What Good Looks Like

Continuous monitoring plan documented in SSP, monitoring frequency proportionate to control risk, automated tools supplement manual monitoring, results compiled in reports, management receives ongoing security posture updates, monitoring outputs feed POAM and risk decisions.

Common Gaps

What assessors actually find in the field:

✗ **No monitoring program**

Between annual assessments, nobody monitors control effectiveness — changes, failures, and new risks go undetected for months.

✗ **Monitoring is manual only**

All monitoring depends on individual attention — no automated tools provide ongoing visibility into log activity or control status.

✗ **No monitoring plan documented**

Monitoring happens informally but no written plan defines which controls are monitored, how often, or by whom.

✗ **Results not reported**

Monitoring activities are conducted by the IT admin but results are never compiled into reports or presented to management.

✗ **Monitoring frequency too low**

Controls are 'monitored' annually during the formal assessment — this does not satisfy the 'ongoing' requirement of this control.