CA.L2-3.12.2

Security Assessment

Operational Plan of Action

"Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems."

Objectives

[a]
Deficiencies and vulnerabilities to be addressed by the plan of action are identified.

[b]
A plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

[c]
The plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Key Discussion Points

Identify First:
[a] requires identifying what goes in the POAM — findings from assessments, vulnerability scans, audits, and self-assessments are all candidates.

Develop the Plan:
[b] requires a written plan — each item needs an owner, milestones, a due date, and a remediation approach. A spreadsheet can qualify.

Execute the Plan:
[c] requires execution — a POAM that exists but is never worked is a finding in itself. Progress and closure must be documented.

Two POAMs Exist:
This operational POAM differs from the CMMC assessment POA&M under 32 CFR 170.21 — the 180-day closeout requirement does not apply here.

Assessment Methods

EXAMINE

Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action.

INTERVIEW

Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities.

TEST

Mechanisms for developing, implementing, and maintaining plan of action.

CA.L2-3.12.2

SECURITY ASSESSMENT — Operational Plan of Action

Plain English

What this control is really saying:

Every assessment, scan, and audit generates findings. This control requires that you do something with them — document each deficiency and vulnerability, create a plan with owners and due dates, and actually execute the plan. A POA&M that sits in a drawer is not compliance.

How it is used:

- Every vulnerability scan, control assessment, and audit finding is entered into the POAM — each item includes the finding, risk level, owner, planned mitigation, and due date.
- The POAM is reviewed monthly — progress against milestones is documented and overdue items are escalated to management.
- When a POAM item is closed, a verification step confirms the fix is effective — a follow-up scan or control test provides closure evidence.
- The POAM is a living document — new findings are added as they are identified and closed items remain for historical record.

Real World Example

The Scenario

Acme Defense completed a vulnerability scan and control assessment last year. The results identified 12 deficiencies. The findings were compiled in a spreadsheet but never formalized into a POAM. No remediation has been assigned or tracked.

What the assessor finds

Eight of the 12 deficiencies are still open one year later. No owner is assigned to any finding. Three findings are now included on the CMMC assessment and the assessor asks for POAM documentation — none exists. The spreadsheet has not been updated since it was created.

SPRS Score Impact

3.12.2 carries a point value of 5. The POAM is the primary evidence that an organization is actively managing its security gaps — assessors look for a current, maintained POAM as a central artifact of program maturity.

What Good Looks Like

POAM maintained with all known deficiencies and vulnerabilities, each item has assigned owner and due date, POAM reviewed and updated regularly, completed items closed with verification evidence, current POAM available as assessment artifact.

Common Gaps

What assessors actually find in the field:

✗ No POAM exists

Vulnerabilities and deficiencies are known but there is no formal plan of action — findings are tracked informally in email threads.

✗ POAM not updated

A POAM was created 18 months ago but has never been updated — completed items are not closed and new findings are not added.

✗ No ownership assigned

POAM items list what needs to be fixed but do not assign a responsible individual — nobody is accountable for remediation.

✗ No due dates

The POAM documents findings but no target remediation dates are set — items sit open indefinitely with no urgency or accountability.

✗ POAM never implemented

A detailed POAM was created following an assessment but no remediation has been performed — the plan exists but is not being executed.