RA.L2-3.11.3

Risk Assessment

Vulnerability Remediation

"Remediate vulnerabilities in accordance with risk assessments."

Objectives

[a]
Vulnerabilities are identified.

[b]
Vulnerabilities are remediated in accordance with risk assessments.

Key Discussion Points

Risk-Based Priority:
Remediation order is driven by risk — CVSS score, active exploitation status, and CISA KEV designation all factor into prioritization.

Track the Open Ones:
Vulnerabilities not yet remediated must be in the POAM — accepting risk informally without documentation is a direct gap in this control.

Verify the Fix:
A patch applied is not a vulnerability closed until verified — a follow-up scan confirming remediation is part of the closure process.

Builds on 3.11.2:
3.11.2 identifies vulnerabilities; 3.11.3 closes them — both must be met and the POAM from CA.L2-3.12.2 is the remediation tracking vehicle.

Assessment Methods

EXAMINE

Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and configuration; vulnerability scanning results; patch and vulnerability management records.

INTERVIEW

Personnel with risk assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for vulnerability scanning, analysis, remediation, and information sharing; mechanisms supporting vulnerability scanning, analysis, and remediation.

RA.L2-3.11.3

RISK ASSESSMENT — Vulnerability Remediation

Plain English

What this control is really saying:

Scanning tells you what's wrong. Remediation is actually fixing it. This control requires that you close vulnerabilities based on risk — critical vulnerabilities first, lower-risk ones on a documented schedule. Vulnerabilities you choose not to remediate must be risk-accepted with documented justification.

How it is used:

- Vulnerability scan results are triaged within 48 hours — critical and high findings are assigned to remediation owners with defined due dates.
- A patch management schedule maps CVSS severity to remediation timelines: Critical = 15 days, High = 30 days, Medium = 90 days, Low = next quarterly cycle.
- Vulnerabilities that cannot be immediately patched are documented in the POAM with a risk acceptance rationale and a planned remediation date.
- Remediation completion is tracked in a vulnerability management log — closed vulnerabilities are verified by a follow-up scan before being marked resolved.

Real World Example

The Scenario

Acme Defense runs monthly vulnerability scans and generates reports. The IT admin reviews scan results but has never remediating any findings — he is waiting for a 'good time' to apply patches that won't disrupt operations. Eighteen months of findings have accumulated.

What the assessor finds

The latest scan shows 23 critical and 47 high vulnerabilities. Several are on the CISA KEV list with known active exploitation. All 23 criticals are unpatched — some have been open for over a year. No POAM entries exist for any of them.

SPRS Score Impact

3.11.3 carries a point value of 5. Open critical vulnerabilities with no remediation plan or POAM entry are among the most impactful findings in a CMMC assessment — active exploitation of known vulnerabilities is the primary attack vector against DIB contractors.

What Good Looks Like

Risk-based remediation timelines defined, scan results reviewed and triaged promptly, critical and high vulnerabilities remediated on schedule, open findings in POAM with risk acceptance documentation, remediation verified by follow-up scan.

Common Gaps

What assessors actually find in the field:

✗ Scan results not acted on

Vulnerability scans are run and reports are generated but nobody reviews them — findings accumulate without triggering any remediation.

✗ No remediation timeline

Vulnerabilities are identified but no policy defines how quickly they must be remediated — findings sit open with no due dates.

✗ Critical vulns not prioritized

Patches are applied by convenience rather than risk — a critical CVE is unpatched while low-severity issues were closed first.

✗ No POAM entries for open vulns

Unpatched vulnerabilities are not tracked in the POAM — there is no documented risk acceptance or planned remediation for open findings.

✗ Remediation not verified

Patches are applied and marked resolved without a follow-up scan — no confirmation that the remediation actually closed the vulnerability.