RA.L2-3.11.2

Risk Assessment

Vulnerability Scan

"Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified."

Objectives

[a]
The frequency to scan for vulnerabilities in organizational systems and applications is defined.

[b]
Vulnerability scans are performed on organizational systems with the defined frequency.

[c]
Vulnerability scans are performed on applications with the defined frequency.

[d]
Vulnerability scans are performed on organizational systems when new vulnerabilities are identified.

[e]
Vulnerability scans are performed on applications when new vulnerabilities are identified.

Key Discussion Points

Two Triggers:
Scheduled scans on a defined frequency AND triggered scans on new vulnerability disclosure — both are required, not one or the other.

All Boundary Assets:
Servers, workstations, laptops, printers, VMs — any device within the CMMC assessment boundary must be in scope, including remote endpoints.

Authenticated Scans:
Unauthenticated scans miss many vulnerabilities — authenticated scanning provides a more complete view of the system's actual exposure.

Current Definitions:
The scanner must use current CVE definitions — an outdated scanner may not detect recently disclosed vulnerabilities relevant to CUI systems.

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.L2-3.11.2

RISK ASSESSMENT — Vulnerability Scan

Plain English

What this control is really saying:

You can't patch what you don't know is broken. Vulnerability scanning systematically identifies weaknesses in your systems and applications before attackers find them. This control requires scheduled scans on a defined frequency AND triggered scans whenever new vulnerabilities are publicly disclosed — both components must be in place.

How it is used:

- Authenticated vulnerability scans run monthly against all CUI workstations, servers, and network devices — scan results are reviewed within 48 hours.
- The vulnerability scanner is configured to pull the latest CVE definitions before each scan — new vulnerabilities are included in the next scheduled scan.
- When a critical CVE is published affecting CUI systems (e.g., CISA KEV), an out-of-cycle scan is triggered within 24 hours — not waiting for the next scheduled scan.
- Scan scope includes all CMMC assessment boundary assets: servers, workstations, laptops, printers, and remote-worker endpoints.

Real World Example

The Scenario

Acme Defense runs vulnerability scans quarterly using a free scanner. The scanner is not authenticated, runs only against the server subnet, and has not been updated in eight months. Workstations and remote-worker laptops are never scanned.

What the assessor finds

A CISA KEV entry published six weeks ago affects all Windows workstations. No out-of-cycle scan was triggered. Two workstations in the CUI environment are unpatched and vulnerable. The quarterly scan would not have caught them anyway — workstations are excluded from the scan scope.

SPRS Score Impact

3.11.2 carries a point value of 3. An unscanned environment has an unknown vulnerability surface — the SPRS score cannot accurately reflect security posture when vulnerabilities remain undiscovered and untracked.

What Good Looks Like

Vulnerability scanning frequency defined in SSP, authenticated scans on all CMMC boundary assets, scanner definitions current, out-of-cycle scans triggered on critical CVE disclosure, scan results documented and used to drive patching and POAM.

Common Gaps

What assessors actually find in the field:

✗ No vulnerability scanner

No automated vulnerability scanner is deployed — vulnerabilities are only discovered after exploitation or when applying patches manually.

✗ Scans not on schedule

The SSP says 'quarterly scans' but the last scan was 14 months ago — no process ensures scans actually happen on the defined schedule.

✗ Unauthenticated scans only

Scans are run without credentials — they miss many internal vulnerabilities that are only visible to authenticated users.

✗ Endpoints not in scope

Servers are scanned but workstations and remote-worker laptops are not included — a large portion of the CMMC boundary is unscanned.

✗ No triggered scans on new CVEs

The organization only scans on schedule — when a critical CVE affecting CUI systems is disclosed, no out-of-cycle scan is performed.