Objectives

[a]
System maintenance is performed.

MA.L2-3.7.1

Maintenance

Perform Maintenance

"Perform maintenance on organizational systems."

Key Discussion Points

All System Types:
Maintenance covers hardware, firmware, and applications — and extends to peripherals like scanners, copiers, and printers.

Four Maintenance Types:
Corrective (fix it), preventative (prevent it), adaptive (environment change), and perfective (improve it) — all four count.

Document Everything:
Maintenance must be logged — who did what, when, on which system. Records support troubleshooting and assessor evidence.

Patching Is Maintenance:
Regular patching is the most common maintenance activity — but it is only one type. Hardware servicing and reconfiguration also apply.

Assessment Methods

EXAMINE

System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan.

INTERVIEW

Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators.

TEST

Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance; mechanisms supporting or implementing controlled maintenance.

MA.L2-3.7.1

MAINTENANCE — Perform Maintenance

Plain English

What this control is really saying:

Unmaintained systems are vulnerable systems. This control requires that you keep your hardware, software, and firmware in good working order — patches applied, hardware serviced, configurations updated. It also requires that maintenance is documented so there is a record of what was done, when, and by whom.

How it is used:

- A maintenance schedule defines patching cycles (monthly OS patches, quarterly firmware), hardware service dates, and annual preventative maintenance windows.
- All maintenance activities are logged in a maintenance record — date, technician name, system affected, work performed, and outcome.
- Vendor-performed hardware maintenance requires the IT admin to be present — maintenance is documented and the system is inspected before returning to service.
- Printers, copiers, and scanners in the CUI environment are included in the maintenance schedule — often overlooked but explicitly covered by this control.

Real World Example

The Scenario

Acme Defense's IT admin applies Windows updates when he remembers, roughly every few months. No formal maintenance schedule exists. A networked multifunction printer in the engineering office has never been updated — it runs firmware from 2019.

What the assessor finds

Three workstations are 147 days behind on patches. The printer firmware has 11 known CVEs including two rated critical. No maintenance log exists. The IT admin cannot produce evidence of any scheduled or completed maintenance activity for the past year.

SPRS Score Impact

3.7.1 carries a point value of 5. Unpatched systems and unmaintained devices are the most direct path for known-vulnerability exploitation — many DIB breaches exploit CVEs for which patches have been available for months or years.

What Good Looks Like

Defined maintenance schedule covering all system types, patches applied on consistent cycle, maintenance activities logged with date and technician, peripheral devices included, vendor maintenance supervised and documented, records retained as evidence.

Common Gaps

What assessors actually find in the field:

✗ **No maintenance schedule**

Systems receive attention only when something breaks — no planned schedule for patching, firmware updates, or hardware service.

✗ **No maintenance records**

Maintenance is performed informally — no log of what was patched, when, or by whom exists as evidence.

✗ **Peripheral devices excluded**

Workstations and servers are maintained but the networked printer and scanner in the CUI environment have never been serviced or patched.

✗ **Vendor access not controlled**

An MSP performs maintenance remotely with no documentation or oversight — no record of what was done during each session.

✗ **Patching inconsistent**

Some systems are regularly patched but others have been missed — no process ensures all systems are covered on the same cycle.