Instructions for SMEs: How to Maintain the Vulnerability & Patch Registers

Version: 1.0

Audience: Small and Medium Enterprises (SMEs), IT Managers, Security Teams

Purpose: Provide simple, repeatable guidance for maintaining the Vulnerability Register and Patch Register.

---

1. Overview

These instructions help SMEs maintain two essential cyber governance records:

1. **Vulnerability Register** – Tracks security weaknesses (CVE findings, misconfigurations, outdated software, etc.).
2. **Patch Register** – Tracks patch updates, deployment status, and compliance for each system.

Maintaining both registers ensures you meet basic cybersecurity expectations, comply with ISO 27001, NIST CSF, and CIS Controls, and reduce overall cyber risk.

---

2. How Often Should Registers Be Updated?

Task	Recommended Frequency
Review new vulnerabilities	Weekly
Update vulnerability statuses	Weekly
Review patch releases (e.g., Patch Tuesday)	Weekly
Update patch deployment progress	Daily/Weekly
Review exceptions & expired waivers	Monthly
Submit compliance report to management	Monthly

---

3. Maintaining the Vulnerability Register

Step 1 — Add Newly Discovered Vulnerabilities

Whenever a vulnerability is identified through:

- Scanners (Nessus, OpenVAS, Qualys)
- CISA KEV alerts
- Vendor bulletins
- IT staff reports
- External assessments

  Add a new row containing:
- Vulnerability ID
- Description
- Asset name
- CVSS score
- Severity
- Exploitability
- Business impact
- Detected date
- Owner and remediation plan

Step 2 — Assign Ownership

Each vulnerability must have a designated owner responsible for remediation.

Step 3 — Prioritise Based on Risk

Use the included **Risk Prioritisation Matrix (Critical/High/Medium/Low)**.

Focus on:

- Critical = fix within **24–72 hours**
- High = fix within **7 days**
- Medium = fix within **30 days**
- Low = fix within **90 days**

Step 4 — Track Progress Until Closure

Update the register as remediation progresses:

- Status (Open, In Progress, Closed)
- Planned remediation date
- Actual remediation date
- Residual risk
- Exceptions (if needed)

Step 5 — Close and Validate

A vulnerability is considered closed when:

- Patch or fix is applied

- Follow-up scans confirm closure
- Documentation is recorded

---

4. Maintaining the Patch Register

Step 1 — Record All Patch Releases

Each month (especially after **Microsoft Patch Tuesday**), list all new patches:

- Patch ID / KB number
- Vendor
- Asset affected
- Severity
- Release date

Step 2 — Plan Deployment

Define:

- Planned deployment date
- Responsible team/owner
- Whether testing is required
- Whether a reboot is required

Step 3 — Record Deployment Activity

During rollout, update the register with:

- Actual deployment date
- Deployment status (Pending / Completed / Failed)
- Testing results
- Rollback availability
- Remediation owner

Step 4 — Track Exceptions

If a patch cannot be applied, document:

- Exception request
- Exception approval
- Compensating controls
- Expiry date

Step 5 — Monthly Patch Compliance Review

Calculate:

- % of endpoints patched
- % of servers patched
- Overdue patches
- Failed deployments
- Reboot compliance

  Submit report to management.

---

5. Recommended Best Practices

✔ Keep Registers in a Central Location

Examples:

- SharePoint
- OneDrive
- Google Drive
- Security folder in GitHub/GitLab (private)

✔ Maintain Version History

Always track changes through:

- Version numbering
- Date stamps
- Change logs

✔ Automate Where Possible

Automation helps reduce human error:

- Export patch reports from Intune/WSUS
- Use vulnerability scanner CSV imports
- Use Python automation scripts (optional)

✔ Keep Ownership Clear

Each row should have a *named* owner.

“No owner” = “Not getting fixed.”

✔ Maintain Executive Visibility

Management should receive:

- Monthly vulnerability overview
- Monthly patch compliance report
- List of overdue risks

This ensures accountability and budget support.

---

6. When to Remove Old Entries

A record can be removed when:

- The vulnerability is verified closed
- The patch is successfully deployed
- Evidence is recorded
- No residual risk remains
- It’s older than **12–18 months** (archive rather than delete)

---

7. Document Control

Version	Date	Author	Notes
1.0	(Insert Date)	(Insert Name)	Initial release