Patch Management Readiness Checklist (Comprehensive)

This checklist helps SMEs measure how prepared they are to execute an effective and repeatable **patch management program**.
Each item should be marked **Yes / No / Partial**.

---

1. Policy & Governance

- □ A documented Patch Management Policy exists.
- □ Policy defines patching timelines (Critical: 24–72 hrs, High: ≤7 days).
- □ Roles & responsibilities for patching are clearly assigned.
- □ Leadership reviews patching performance quarterly.
- □ There is an exception/waiver process for delayed patches.
- □ Patch approval workflows are documented.

---

2. Asset & Software Inventory

- □ Up-to-date inventory of all endpoints exists.
- □ Software inventory includes versions, publishers, and install dates.
- □ Unsupported OS/software is identified and risk-assessed.
- □ All externally facing systems are catalogued.
- □ Cloud workloads (VMs, containers, apps) are inventoried.

---

3. Patch Deployment Processes

- □ A weekly or monthly patch cycle exists and is followed.
- □ Emergency patches have a fast-track process.
- □ Patches are tested before deployment (pilot group).
- □ All machines receive updates automatically OR via management tool.
- □ Pending reboots are tracked and enforced.
- □ Third-party patching (Chrome, Adobe, Java, etc.) is included.

---

4. Technical Controls & Automation

- □ Windows Update for Business / WSUS / Intune / RMM is configured.
- □ Linux package updates are managed centrally.
- □ Applications are configured for auto-update where possible.
- □ Scripts or tools validate patch installation success.
- □ Endpoint protection alerts for missing patches.

---

5. Coverage & Compliance

- □ ≥ 90% of endpoints meet patching timelines.
- □ ≥ 90% of servers meet patching timelines.
- □ Mobile devices (iOS/Android) are included in patch compliance.
- □ Remote/hybrid users receive patches via VPN/Cloud management.
- □ Compliance dashboards exist (Intune/WSUS/Excel/Custom).

---

6. Vulnerability & Threat Intelligence Integration

- □ Patch prioritisation includes risk (CVSS + exploitability).
- □ CISA KEV (Known Exploited Vulnerabilities) list is monitored.
- □ Microsoft Patch Tuesday summaries are reviewed.
- □ External vulnerability scans inform patch priorities.
- □ Zero-day alerts trigger immediate assessment.

---

7. Monitoring & Reporting

- □ Patch results are logged and stored for at least 12 months.
- □ Weekly or monthly reports are generated automatically.
- □ Failures are flagged and reattempted promptly.
- □ High-risk or overdue patches are escalated to management.
- □ Patch performance KPIs: MTTR, compliance %, failure rate.

---

8. Change Control & Testing

- □ A change control process exists for patch rollouts.

- □ Patch rollback plan exists and is tested.
- □ Backups are verified before patch deployment.
- □ Critical systems undergo test deployment first.
- □ Maintenance windows are scheduled and communicated.

---

9. Cloud & SaaS Workloads

- □ M365 Secure Score patch-related items are monitored.
- □ AWS Inspector / Azure Defender scans are reviewed.
- □ Cloud OS images (golden images) are regularly updated.
- □ SaaS vendor patch cadences are reviewed annually.

---

10. Continuous Improvement

- □ Patch performance is reviewed quarterly.
- □ Lessons learned sessions are conducted annually.
- □ Patching timelines are adjusted based on threat activity.
- □ Repeated failures trigger root-cause analysis.

Summary Score (Optional)

Mark each item as Yes (1), Partial (0.5), No (0).
Total score = overall readiness (Max = 50+).

Use this checklist to:

- Measure patching maturity
- Prioritise improvements
- Support ISO 27001 / NIST CSF / CIS v8 controls