# Vulnerability Management Questionnaire (Comprehensive)

This questionnaire helps small and medium-sized organisations assess their current vulnerability and patch management posture.

Score each question from **0 to 3**:

- **0 = Not implemented**
- **1 = Partially implemented**
- **2 = Mostly implemented**
- **3 = Fully implemented**

---

## 1. Governance & Policy

1. Do you have a documented Vulnerability Management Policy?
2. Does your policy mandate regular vulnerability scanning?
3. Is there a formally assigned vulnerability management owner?
4. Are roles/responsibilities clearly documented?
5. Are patching timelines defined based on severity?
6. Does management review the policy at least annually?
7. Is there an exception/waiver process for delayed patching?

---

## 2. Asset Inventory & Classification

8. Do you maintain an up-to-date inventory of all endpoints?
9. Are servers, workstations, and cloud assets classified by criticality?
10. Is asset ownership defined for each system?
11. Are externally exposed systems identified and tracked?
12. Do you maintain a software inventory (applications, versions)?
13. Do you track unsupported/legacy systems?

---

## 3. Vulnerability Scanning & Tools

14. Do you run authenticated vulnerability scans?

15. Are scans performed at least monthly?
16. Do you scan internet-facing systems weekly or more?
17. Do you use more than one scanning method (agentless/agent-based)?
18. Are vulnerability scan results archived for at least 12 months?
19. Are high-severity vulnerabilities automatically flagged?

---

# 4. Patch Management Process

20. Do you have a documented patch management procedure?
21. Are patches applied based on risk (CVSS + business impact)?
22. Are emergency patches handled within 24–72 hours?
23. Do you test patches before deployment?
24. Do you maintain a weekly or monthly patch cycle?
25. Do systems automatically install updates when applicable?
26. Do you track pending reboots?

---

# 5. Configuration & Baseline Security

27. Do you have a secure baseline for Windows systems?
28. Are CIS/Benchmarks partially or fully implemented?
29. Do you enforce TLS 1.2/1.3 on servers?
30. Do you check for weak ciphers?
31. Do you check systems for disabled ASLR/DEP/CFG?
32. Are browser security settings hardened?

---

# 6. Endpoint & Server Patch Coverage

33. Are Windows endpoints ≥90% patched within required timelines?
34. Are servers ≥90% patched within required timelines?
35. Do you track patching failures?
36. Do you maintain patch compliance dashboards?
37. Do you verify patching success (not just deployment)?

---

# 7. Cloud & SaaS Security (M365, AWS, etc.)

38. Are cloud workloads scanned for vulnerabilities?
39. Do you monitor M365 Secure Score relevant to patching?

40. Do you track outdated OS versions on cloud VMs?
41. Do you verify SaaS vendor patch cadence?

---

# 8. Vulnerability Triage & Prioritisation

42. Do you prioritise vulnerabilities based on exploitability?
43. Do you map vulnerabilities to business-critical systems?
44. Are exploit trends monitored (CISA KEV, MS bulletins)?
45. Are long-standing vulnerabilities escalated to management?

---

# 9. Reporting & Metrics

46. Do you produce regular vulnerability reports (weekly/monthly)?
47. Do you measure MTTR (mean time to remediate)?
48. Do you measure patch compliance percentages?
49. Are unresolved critical vulnerabilities escalated?

---

# 10. Continuous Improvement

50. Do you perform annual vulnerability management reviews?
51. Do you conduct penetration tests or external assessments?
52. Do you adjust patch timelines based on threat environment?
53. Do you track false positives and recurring weaknesses?
54. Are lessons learned fed back into the patching process?

---

## Scoring Summary

- **0–40 = Very Low Maturity**
- **41–80 = Low Maturity**
- **81–120 = Moderate Maturity**
- **121–162 = High Maturity**

Use this questionnaire to:

- Identify weaknesses
- Prioritise improvements
- Build patch governance maturity