Mapping to Standards: Vulnerability & Patch Management

Version: 1.0

Purpose: This document maps the Vulnerability & Patch Management Toolkit to relevant cybersecurity standards and frameworks used globally, ensuring compliance for SMEs.

---

1. ISO 27001:2022 Mapping

A.12.6 – Technical Vulnerability Management

Toolkit Component	Standard Requirement
Vulnerability Management Policy	Requires documented approach for technical vulnerabilities
Vulnerability Register	Tracking discovered vulnerabilities
Risk Prioritisation Matrix	Assessment to determine risk and prioritisation
Patch Management SOP	Procedures for timely application of patches
Exception & Risk Acceptance Form	Controlled risk acceptance process
Monthly Compliance Reporting	Ongoing monitoring and review

A.8 – Asset Management

Toolkit Component	Standard Requirement
Asset fields in Registers	Assets must be identified and managed
Criticality ratings	Classification of asset importance

A.5.23 – Information Security in the Use of Cloud Services

Toolkit Component	Standard Requirement
Cloud patching steps	Ensures cloud assets are patched and monitored
Cloud vulnerability scanning	Reference to AWS Inspector / Azure Defender

---

2. NIST Cybersecurity Framework (NIST CSF) Mapping

Identify (ID)

Subcategory	Toolkit Component
ID.AM-1: Asset inventory	Vulnerability & Patch Registers
ID.RA-1: Asset vulnerabilities identified	Vulnerability management questionnaire

Protect (PR)

Subcategory	Toolkit Component
PR.IP-12: A vulnerability management plan is developed and implemented	Policies + SOPs
PR.MA-1: Maintenance and repair performed	Patch deployment workflow

Detect (DE)

Subcategory	Toolkit Component
DE.CM-8: Vulnerability scanning	Vulnerability scanning and intake process

Respond (RS)

Subcategory	Toolkit Component
RS.MI-1: Mitigation performed	Patch duties, testing, deployment

---

3. CIS Controls v8 Mapping

Control 7 – Continuous Vulnerability Management

Toolkit Component	Requirement
Vulnerability Register	Track identified vulnerabilities
Risk Matrix	Prioritise vulnerabilities
Scanner outputs	Routine scanning
Questionnaire	Assess readiness and process maturity

Control 4 – Secure Configuration of Enterprise Assets

Toolkit Component	Requirement
Patch SOP	Establish, implement, and maintain secure configurations
TLS Baseline	Enforce secure protocols

Control 16 – Application Software Security

Toolkit Component	Requirement
Patch workflow	Ensure applications are updated and secure

---

4. Cyber Essentials (UK)

CE Control 2: Secure Configuration

- Patch Management SOP ensures systems are securely configured.

CE Control 3: Software Updates

- Patch Register and SOP ensure timely software updates.

CE Control 4: Malware Protection

- Indirectly supported by patching critical vulnerabilities.

CE Control 5: Firewalls & Internet Gateways

- TLS & network misconfiguration scanning aligns with secure boundary defence.

---

5. SOC 2 (Security Trust Principle)

CC7.1 – Vulnerabilities Remediated

Toolkit Component
Patch Register
Vulnerability Register
Monthly Compliance Reporting

CC8.1 – Change Control

Toolkit Component
Change Control Form
Patch Testing Log (optional)

---

6. HIPAA (Security Rule) — Technical Safeguards

164.308(a)(8): Evaluation

- Vulnerability assessments part of periodic evaluation.

164.308(a)(1)(ii)(B): Risk Management

- Risk prioritisation matrix supports documenting and reducing risks.

---

7. Document Control

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