SECURITY • AUDIT + HARDENING

Website Security Audit Checklist

A practical, agency-ready checklist to reduce common website risks and improve resilience.

Malaysia edition

Prepared for Malaysian SMEs & corporates | Updated 2026-04-22

Table of Contents

How to use this ebook

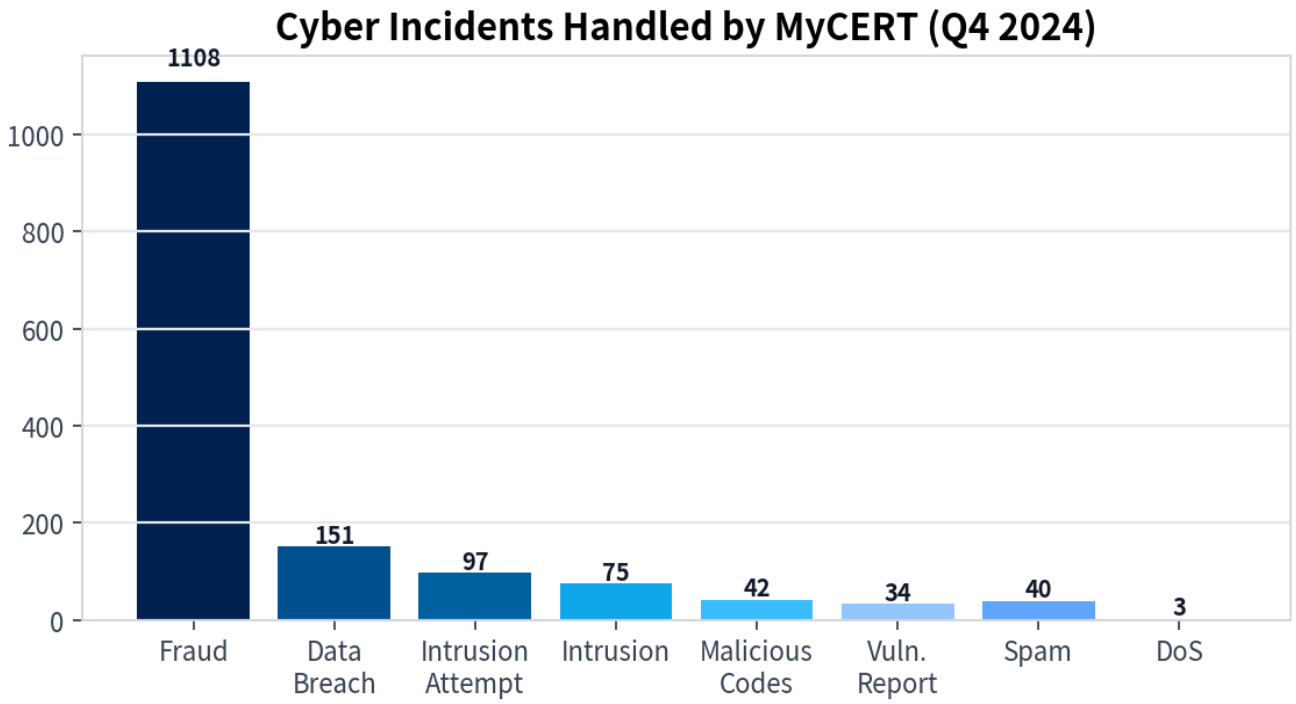
Skim the executive summary first, then jump to the checklists and templates. Use the charts to align decisions with realistic KPIs and timelines.

01 Executive Summary

Q4 2024	71%	MFA	Backups
MyCERT report	**Fraud share**	**Priority 1**	**Priority 2**
local incident trends	of reported incidents	reduce account takeovers	restore tested

Most website compromises are basic: weak passwords, outdated plugins, missing backups, and misconfigurations. A recurring audit cadence prevents most incidents.

02 Malaysia Threat Snapshot



Incidents handled by MyCERT (Q4 2024). Fraud dominates the mix.

Phishing reality

MyCERT reported phishing as the top fraud type in Q4 2024. Treat phishing resistance (MFA, training, verification steps) as a core business control.

03 Security Audit Checklist (Agency Standard)

Category	Check	Status
Access	Admin accounts reviewed; remove ex-staff	
Access	MFA enabled for admin, hosting, DNS, email	
Patching	CMS/core + plugins/themes updated	
Backups	Automated backups + restore test done	
Transport	HTTPS enforced; HSTS where possible	
AppSec	Input validation; protect against XSS/SQLi	
Monitoring	Alerts for suspicious admin logins	
Resilience	Incident response steps documented	

OWASP Top 10 mapping

Use OWASP Top 10 as a baseline for common web risks. Even for WordPress sites, many OWASP failures show up as misconfiguration, weak access control, and vulnerable components.

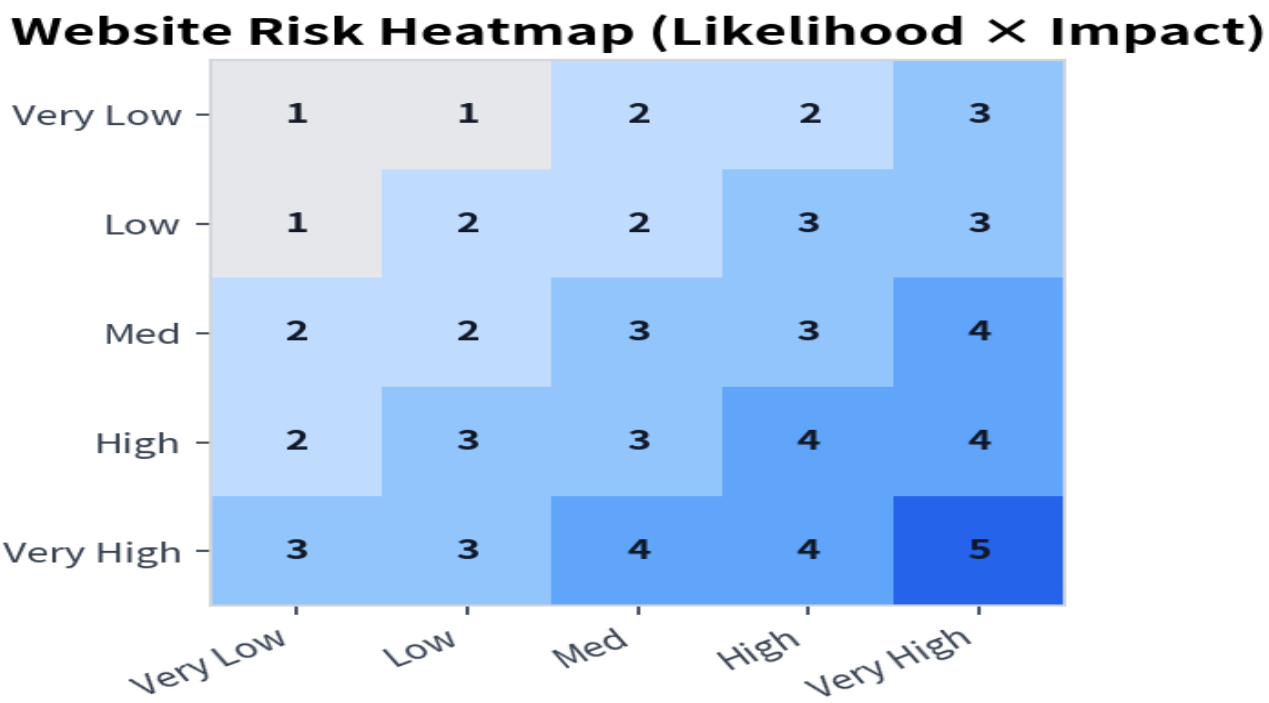
04 Security Headers Checklist

Header	Why it matters
Content-Security-Policy (CSP)	Reduces XSS risk by controlling allowed scripts
Strict-Transport-Security (HSTS)	Forces HTTPS to prevent downgrade attacks
X-Content-Type-Options	Prevents MIME sniffing issues
Referrer-Policy	Limits referrer leakage
Permissions-Policy	Restricts sensitive browser APIs

Important

Test headers carefully to avoid breaking site functionality. Consider CSP report-only mode first.

05 Risk Heatmap + Prioritisation



Use a risk heatmap to prioritise fixes: address high-likelihood/high-impact items first.

Top risks (typical)	Quick controls
Credential theft / phishing	MFA + least privilege + verification steps
Outdated plugins	Patch schedule + remove unused components
No backups	Automated backups + quarterly restore drill
Misconfiguration	Security headers + locked-down admin endpoints
No monitoring	Login alerts + uptime + file integrity checks

06 CMS / WordPress Hardening (If applicable)

- Remove unused plugins/themes; fewer components = fewer vulnerabilities.
- Disable default admin usernames; enforce strong passwords + MFA.
- Limit login attempts; add CAPTCHA where appropriate.
- Use least privilege: editors should not be admins.
- Keep server/runtime versions supported and patched.

> **Backup rule**
>
> A backup you have never restored is not a backup. Schedule a full restore test at least quarterly.

07 Phishing & Staff Controls

Given the dominance of phishing-related fraud, treat staff controls as part of your website security posture.

Control	Implementation
MFA everywhere	Email, hosting, DNS, CMS admins
Verification steps	Call-back rule for payment detail changes
Password manager	Company-managed vault for shared access
Access offboarding	Disable accounts immediately on staff exit

08 Vendor & SLA Checklist

Question	Why it matters
Who owns domains and hosting logins?	Avoid lockouts; you must control critical assets
Patch responsibility?	Define who updates CMS/plugins and when
Backup responsibility?	Define frequency and restore support
Incident response time?	Know what happens after-hours
Logs and monitoring?	Needed for investigations and prevention

Talk to JOeve Smart Solutions

If you want implementation support (strategy → build → optimisation), start here:
https://www.joevesmartsolutions.com/contact

09 Audit Cadence + Incident Mini-Plan

Frequency	Actions
Weekly	Updates + alert review + uptime checks
Monthly	User access review + malware scan + restore test (spot)
Quarterly	Headers/vuln scan + full restore test (staging)
Annually	Pen test (as needed) + disaster recovery drill

Incident step	What to do
Contain	Lock accounts, revoke tokens, take site offline if needed
Preserve	Save logs, timestamps, suspicious files
Investigate	Identify entry point (plugin/credentials/server)
Recover	Restore from clean backup, patch, rotate credentials
Notify	Inform stakeholders/customers if data may be affected

Talk to JOeve Smart Solutions

If you want implementation support (strategy → build → optimisation), start here:
https://www.joevesmartsolutions.com/contact

Sources & Notes

This ebook references publicly available sources. Figures may change over time; verify critical numbers before making investment decisions.

- **CyberSecurity Malaysia - MyCERT Q4 2024 incident report**: https://www.cybersecurity.my/portal-main/advisories-details/e14a3424-f7d4-11ef-9a4c-005056812d51
- **OWASP Top Ten**: https://owasp.org/www-project-top-ten/
- **JOeve - Privacy Policy (PDPA)**: https://www.joevesmartsolutions.com/privacy

> **More free resources**
>
> Download more at: https://www.joevesmartsolutions.com/resources

Ready to scale with AI + digital?

Get a personalised strategy for your business in Malaysia.

Contact JOeve Smart Solutions
Email: thomas@joevesmartsolutions.com
Phone: +6016 557 2800 | Penang, Malaysia
Website: https://www.joevesmartsolutions.com/contact
Explore services: AI chatbots, SEM, landing pages, web apps, and automation.