

FREE RESOURCE

CMS Security Checklist

7 questions every organisation should be able to answer about their website CMS.

Use this checklist with your web team, digital agency, or IT manager. For each item, note your status in the **Status / Notes** column. Any “No” or “Unsure” answer represents an exposure worth addressing.

1 Is my CMS on a currently supported version?

HIGH

Vendor is actively shipping security patches for your version. If your CMS is end-of-life or approaching EOL, this is your highest priority item.

☐ Yes ☐ No ☐ Unsure

2 Is the latest security patch installed?

HIGH

Your CMS should be on the most recent release of its current supported version. Check your CMS admin panel or ask your agency.

☐ Yes ☐ No ☐ Unsure

3 Have all plugins and modules been audited and updated?

HIGH

Plugins are the most common attack vector in CMS exploitation campaigns. Every unupdated plugin is a potential entry point.

☐ Yes ☐ No ☐ Unsure

4 Are CMS admin accounts protected by MFA?

HIGH

Multi-factor authentication should be mandatory for all administrator and editor accounts. A compromised admin credential without MFA is game over.

☐ Yes ☐ No ☐ Unsure

5 **Is a Web Application Firewall (WAF) in place?**

MEDIUM

A WAF filters malicious traffic before it reaches your CMS. Not a substitute for patching, but a meaningful additional layer.

☐ Yes ☐ No ☐ Unsure

6 **Have hosting and server configurations been recently reviewed?**

MEDIUM

Web directories should be configured as read-only where possible. Server-side execution in upload directories is a known webshell deployment vector.

☐ Yes ☐ No ☐ Unsure

7 **Are backups automated, tested, and stored off-site?**

MEDIUM

If a webshell is deployed and your site is compromised, recovery depends on having a clean, recent backup that wasn't on the compromised server.

☐ Yes ☐ No ☐ Unsure

Two additional questions for platforms approaching end of life

8 **When does my CMS version reach end of support?**

HIGH

Find your platform's official EOL date. Build it into your IT and budget planning. Waiting until EOL arrives to start planning is the most common mistake.

☐ Yes ☐ No ☐ Unsure

9 **Is a migration plan in place before EOL?**

HIGH

A migration from an EOL platform takes time – typically 3–6 months for a mid-sized site. If your EOL date is within 12 months, the planning conversation should already be underway.

☐ Yes ☐ No ☐ Unsure

How to use your results

ALL YES

Good posture. Review this checklist every 6 months and after any major CMS or plugin update.

1-2 NO

Manageable. Prioritise the High-risk items first. Get a timeline from your agency for remediation.

3+ NO

Elevated risk. Especially if any High-risk items are unanswered. Escalate to your IT lead or digital agency this week.

Need help working through the checklist?

[Dapth](#) is a perth based digital agency and Kentico Gold Partner. We help organisations assess CMS security posture, plan platform migrations, and build on modern, supported web infrastructure.

[Talk to Dapth →](#)