CLOUDWATCH SOLUTIONS

27-Point Website & Infrastructure Health Checklist

The list we work through before taking over any website or server. Twenty-seven yes/no questions across ownership, backups, monitoring, server health, security, WordPress and performance — each with what to check, why it matters, and the answer that should worry you.

How to use it

1. Work through all 27 points before fixing anything. Mark each one Yes, No, or Don’t know.
2. A “Don’t know” is a finding. Not knowing whether backups restore, or who owns the domain, is the same as it being broken — you just haven’t found out yet.
3. Then fix in this order: backups, then access and ownership, then updates, then monitoring. Those four remove most of the ways a website turns into an emergency.

What’s covered

Ownership & access
Items 1–5

Backups, recovery & monitoring
Items 6–11

Server & platform
Items 12–16

Edge & security
Items 17–23

WordPress & email
Items 24–25

Performance & accessibility
Items 26–27

Version 2026-09. The current version, with a working copy you can tick off in the browser, is always at cloudwatchsolutions.com/website-health-checklist/

OWNERSHIP & ACCESS

Ownership & access

Everything else on this list is fixable. Losing control of the domain, the DNS or the hosting account is not. Start here.

☐ 1 You control the domain registrar account

WHAT TO CHECK

You (not an agency, not a former employee) can log in to the registrar. Auto-renew is on, the domain is locked against transfer, and the contact email is one you read.

WHY IT MATTERS

Expired or hijacked domains take the website, email and every login reset with them. Recovery can take weeks and is not guaranteed.

Red flag: "Our old web guy set that up."

☐ Yes ☐ No ☐ Don't know

☐ 2 DNS is hosted somewhere you can log into, and the records are documented

WHAT TO CHECK

You know which service answers DNS for the domain (registrar, Cloudflare, host) and have the login. Every record has a known purpose; nothing points at a server that no longer exists.

WHY IT MATTERS

Stale records are how a forgotten subdomain becomes a phishing page, and undocumented records are why migrations break email.

Red flag: Records nobody can explain, or a DNS provider nobody can access.

☐ Yes ☐ No ☐ Don't know

☐ 3 The TLS certificate is valid, automatic and complete

WHAT TO CHECK

HTTPS works on both the bare domain and www, HTTP redirects to HTTPS, the certificate renews itself, and no page loads mixed (insecure) content.

WHY IT MATTERS

An expired certificate is a full outage in every browser. Manual renewal is a reminder somebody eventually misses.

Red flag: A calendar entry to renew the certificate.

☐ Yes ☐ No ☐ Don't know

☐ 4 You know who hosts the site, what you pay, and who holds the login

WHAT TO CHECK

The hosting company, plan, renewal date and account owner are written down. You can add and remove people's access yourself.

WHY IT MATTERS

When something breaks at 9pm, the first question is always "where does this run and who can get in".

Red flag: Hosting billed through a third party you can't reach directly.

☐ Yes ☐ No ☐ Don't know

☐ 5 There is one document listing every account and who has access

WHAT TO CHECK

Registrar, DNS, hosting, CDN/Cloudflare, email, analytics, premium plugin licences, payment gateways: each with owner, access list and renewal date. Reviewed at least yearly.

WHY IT MATTERS

This is the difference between a two-hour handover and a two-month archaeology project when a provider or employee leaves.

Red flag: It lives in someone's head, or in a departed contractor's inbox.

☐ Yes ☐ No ☐ Don't know

BACKUPS, RECOVERY & MONITORING

Backups, recovery & monitoring

Most website emergencies are not caused by attackers. They are caused by an update, a full disk or a bad change, with no way back.

☐ 6 Backups run automatically and are stored off the server

WHAT TO CHECK

Files and database are backed up at least daily (more often if the site changes more often), copied to different storage than the server itself, and kept for 30 days or more.

WHY IT MATTERS

A backup on the same disk as the site disappears with the site. A backup from last quarter restores last quarter's orders.

Red flag: "The host does backups" — with no idea where they are or how far back they go.

☐ Yes ☐ No ☐ Don't know

☐ 7 A restore has actually been tested

WHAT TO CHECK

Someone has restored a backup to a test location in the last six months, confirmed the site worked, and knows roughly how long it took.

WHY IT MATTERS

Backups that have never been restored are a hope, not a plan. Corrupt archives, missing tables and missing uploads only show up on restore day.

Red flag: The last restore was never.

☐ Yes ☐ No ☐ Don't know

☐ 8 There is a written recovery plan for the likely disasters

WHAT TO CHECK

Short, plain-language steps for: the server dies, the site is hacked, the domain lapses, the hosting provider disappears. Each names who acts and how long the business can tolerate being down.

WHY IT MATTERS

Decisions made during an outage are worse and slower than decisions made in advance.

Red flag: "We'd call someone."

☐ Yes ☐ No ☐ Don't know

☐ 9 External uptime monitoring alerts a human

WHAT TO CHECK

A service outside your hosting checks the site every 1–5 minutes, verifies real page content (not just a 200 status), and alerts a phone — not only an inbox.

WHY IT MATTERS

Without it, customers find outages before you do. With it, you often fix them before customers notice.

Red flag: You learned about the last outage from a customer.

☐ Yes ☐ No ☐ Don't know

☐ 10 A staging copy exists for testing changes

WHAT TO CHECK

There is a non-public copy of the site where updates, new plugins and design changes are tried before they reach production.

WHY IT MATTERS

Every update is a change to running code. Testing it against a copy is the cheapest insurance there is.

Red flag: Updates are applied straight to the live site and "we watch for problems".

☐ Yes ☐ No ☐ Don't know

☐ 11 Updates follow a procedure, on a schedule, with an owner

WHAT TO CHECK

A named person applies updates at a known cadence, takes a backup first, tests on staging, and checks key pages afterwards. Security updates are handled faster than feature updates.

WHY IT MATTERS

Unpatched software is how most sites get compromised; careless patching is how most sites get broken. A procedure fixes both.

Red flag: Updates happen "when someone remembers" or never.

☐ Yes ☐ No ☐ Don't know

SERVER & PLATFORM

Server & platform

Slow sites and sudden outages usually trace back to a handful of unglamorous things: resource headroom, PHP configuration, the database, and caching that isn't actually working.

☐ 12 Resource headroom is known and alerted on

WHAT TO CHECK

You know the server's CPU, memory and disk usage at a normal peak. Disk stays below ~80%. Someone is alerted before memory or disk run out, not after.

WHY IT MATTERS

A full disk breaks logins, uploads and the database in confusing ways. Memory exhaustion is the most common cause of "the site just went down for no reason".

Red flag: No graphs, no alerts, or a disk already over 90%.

☐ Yes ☐ No ☐ Don't know

☐ 13 PHP is a supported version and PHP-FPM is sized for the traffic

WHAT TO CHECK

The PHP version still receives security updates. The PHP-FPM pool (worker count, memory per worker) matches the server's RAM and real traffic, and PHP errors are logged somewhere reviewable.

WHY IT MATTERS

Too few workers and requests queue up under load; too many and the server swaps. Both look like "the site is slow sometimes".

Red flag: PHP-FPM settings have never been changed from the defaults, or the PHP version is end-of-life.

☐ Yes ☐ No ☐ Don't know

☐ 14 The database is healthy and its size is known

WHAT TO CHECK

MySQL/MariaDB is a supported version, the database size is known and reasonable, the WordPress options table isn't bloated with autoloaded data, and slow queries can be identified.

WHY IT MATTERS

Database problems are usually gradual (growing tables, transients, logs) and then sudden (timeouts, lock waits, full disk).

Red flag: Nobody has looked at the database since the site launched.

☐ Yes ☐ No ☐ Don't know

☐ 15 Caching is configured and verifiably working

WHAT TO CHECK

Full-page caching for anonymous visitors, an object cache if the site is dynamic or busy, and sensible browser-cache headers for static files. Verified with response headers, not just a plugin that says "enabled".

WHY IT MATTERS

Caching is the difference between a server that handles a traffic spike and one that falls over. Misconfigured caching also causes stale content and broken carts.

Red flag: Two caching plugins active, or a cache plugin installed but every page still hits PHP.

☐ Yes ☐ No ☐ Don't know

☐ 16 Logs are retained, rotated and reviewable

WHAT TO CHECK

Web server, PHP and application logs are kept for at least 14–30 days, rotated so they can't fill the disk, and someone knows where they are.

WHY IT MATTERS

After an incident, logs are how you find out what happened. Without them you are guessing, and you can't tell if it will happen again.

Red flag: Logging disabled "to save space", or logs that have filled the disk.

☐ Yes ☐ No ☐ Don't know

EDGE & SECURITY

Edge & security

A business website is attacked constantly by automated tools, regardless of how small the business is. The goal is to make the site an unrewarding target and to notice when something gets through.

☐ 17 Static assets are served through a CDN

WHAT TO CHECK

Images, scripts and stylesheets are delivered from a CDN edge close to the visitor, with cache rules you understand and can purge.

WHY IT MATTERS

Reduces load on the origin server and makes the site faster for visitors who aren't near your data center.

Red flag: Every image on every page is served directly by the origin server.

☐ Yes ☐ No ☐ Don't know

☐ 18 Cloudflare (or equivalent) is correctly configured

WHAT TO CHECK

DNS records for the site are proxied, SSL mode is Full (strict), and the origin server only accepts traffic from the proxy — so protection can't be bypassed by hitting the server IP directly.

WHY IT MATTERS

A proxy that can be bypassed provides the feeling of protection without the protection.

Red flag: Cloudflare is "on" but the origin IP is public and answers directly.

☐ Yes ☐ No ☐ Don't know

☐ 19 A WAF and rate limiting protect the application

WHAT TO CHECK

Managed WAF rules are enabled, login and XML-RPC endpoints are rate limited, and obviously malicious traffic is challenged or blocked before it reaches PHP.

WHY IT MATTERS

Most attacks are noisy and automated. A WAF stops the bulk of them at the edge, so the server's resources go to real visitors.

Red flag: Thousands of login attempts a day reaching the server unchallenged.

☐ Yes ☐ No ☐ Don't know

☐ 20 Admin access is hardened

WHAT TO CHECK

No account named "admin", strong unique passwords, as few administrator accounts as possible, former staff removed, login attempts limited, and XML-RPC disabled unless something needs it.

WHY IT MATTERS

Credential stuffing and brute force are cheap for attackers. The admin panel is the most valuable door on the site.

Red flag: Six administrators, two of whom nobody recognises.

☐ Yes ☐ No ☐ Don't know

☐ 21 Multi-factor authentication is on for every critical account

WHAT TO CHECK

MFA is enabled on the registrar, DNS, hosting, Cloudflare, email admin and the website admin — for every person with access.

WHY IT MATTERS

A leaked or reused password is the most likely way any of these accounts is taken over. MFA turns that from a takeover into a failed login.

Red flag: MFA is "on the important ones", meaning some.

☐ Yes ☐ No ☐ Don’t know

☐ 22 Malware and file-integrity scanning run on a schedule

WHAT TO CHECK

A server-level scan (not only a plugin inside WordPress) runs regularly, core files are checked against known-good versions, and someone is told when something changes unexpectedly.

WHY IT MATTERS

Compromised sites are usually discovered late — by Google, a customer or a blacklist. Scanning turns that into an early, quiet notification.

Red flag: The only scanner is a plugin that the malware can disable.

☐ Yes ☐ No ☐ Don’t know

☐ 23 Known vulnerabilities in plugins, themes and core are tracked

WHAT TO CHECK

Installed software is checked against a vulnerability feed, and there is an alert (and a fast-track update path) when something in use gets a published CVE.

WHY IT MATTERS

Attackers automate exploitation within hours of a disclosure. Knowing the same day is the difference between patching and cleaning up.

Red flag: You’d find out about a plugin vulnerability when the site is defaced.

☐ Yes ☐ No ☐ Don’t know

WORDPRESS & EMAIL

WordPress & email

The application layer is where most of the day-to-day risk lives: outdated or abandoned software, and email that quietly stops arriving.

☐ 24 **Core, plugins and themes are current, licensed and pruned**

WHAT TO CHECK

Everything is on a supported version, premium licences are valid (so updates arrive), unused plugins and themes are deleted rather than deactivated, and nothing installed has been abandoned by its author.

WHY IT MATTERS

Every installed plugin is code that can be exploited whether or not it’s active. Abandoned plugins never get fixed.

Red flag: A plugin last updated years ago, or an expired licence that has silently stopped updates.

☐ Yes ☐ No ☐ Don’t know

☐ 25 **Email from the site is authenticated and actually delivered**

WHAT TO CHECK

Transactional email (forms, orders, password resets) is sent via an SMTP or API service rather than the server’s mail function. SPF, DKIM and DMARC are published for the domain. A test message lands in the inbox, not spam.

WHY IT MATTERS

Unauthenticated email from a web server is increasingly rejected outright. The failure is silent: forms "work" and nobody receives them.

Red flag: Contact form submissions that "sometimes don’t come through".

☐ Yes ☐ No ☐ Don’t know

PERFORMANCE & ACCESSIBILITY

Performance & accessibility

What the visitor experiences. These two checks are the ones customers and search engines both notice.

☐ 26 **Key pages pass Core Web Vitals**

WHAT TO CHECK

The homepage and top landing pages have acceptable Largest Contentful Paint, interaction responsiveness and layout stability, measured with real-user or lab tools. Time-to-first-byte is reasonable.

WHY IT MATTERS

Slow pages lose visitors before they read anything, and search rankings account for it.

Red flag: Nobody has measured it, or the measurement is from the launch.

☐ Yes ☐ No ☐ Don’t know

☐ 27 **The site works on a phone and for people using assistive technology**

WHAT TO CHECK

Pages are usable on a small screen without zooming, images are sized for mobile, tap targets are large enough, headings are structured, images have alt text, contrast is adequate, and the site can be navigated by keyboard.

WHY IT MATTERS

Most visitors are on phones; some visitors use screen readers. Both are customers, and accessibility failures carry legal exposure in many places.

Red flag: It was only ever tested on the designer’s laptop.

☐ Yes ☐ No ☐ Don’t know

NEXT STEP

Want a second set of eyes on your setup?

If you finished with a few “No”s and “Don’t know”s, that is normal — most businesses do. The harder question is which ones actually matter for your business and what it would take to fix them.

CloudWatch Solutions runs this review against real setups: hosting, WordPress configuration, server resources, Cloudflare / CDN / WAF, backups, monitoring, performance, security and overall infrastructure architecture. You get a short written report of what we found and what we would do first — whether you fix it yourself, hand it to your own IT, or ask us to.

Request a website & infrastructure review

cloudwatchsolutions.com/contact-us/#review · info@cloudwatchsolutions.com · +1 734 363 8831

Keep the checklist current

Subscribers to the Infrastructure Brief get one practical email a week on hosting, WordPress, Cloudflare, AWS, backups and monitoring — and the updated checklist whenever it changes. Sign up at cloudwatchsolutions.com/newsletter/