Cyber Essentials: readiness checklist

The five control areas mapped to a Laravel application on AWS provisioned through Laravel Forge, plus laptops. What to have in place, what evidence to keep, and how to answer the self-assessment. Cyber Essentials is the certificate UK construction, facilities management and public-sector buyers ask for most often, and it is the cheapest item on the whole procurement list.

What you are applying for, and what it costs

ITEM	POSITION AS AT 28 AUGUST 2026
Scheme owner	The National Cyber Security Centre owns the scheme. **IASME** is the sole delivery partner and licenses the certification bodies that mark your submission.
Current question set	**Danzell**, version 16.3 (May 2026), in effect for assessment accounts created **on or after 27 April 2026**. Accounts created before that date continue on the previous set, **Willow**. The question set is published free by IASME, so you can read every question before you pay.
Current requirements document	**Cyber Essentials: Requirements for IT Infrastructure, version 3.3** (April 2026), effective 27 April 2026. This is the document the assessor marks you against. Read it once, end to end; it is 25 pages.
Fee, by organisation size	**Micro, 0 to 9 staff: £320 + VAT.** Small, 10 to 49: £440 + VAT. Medium, 50 to 249: £500 + VAT. Large, 250+: £600 + VAT. TeamTalk is in the micro band.
Cyber Essentials Plus	Price is **not published**: it is quoted individually by a certification body on the size and complexity of the network. Budget [£1,400 to £2,500] for a company this size GET THREE QUOTES. To avoid repeating the self-assessment you must certify to Plus **within three months** of passing the basic assessment. Do this only when a named deal is gated on it in writing.
Validity and renewal	Certificates expire after **12 months**. Renewal is a **full re-assessment, not a light-touch renewal**: you re-enter every answer, and the questions may have changed. IASME reminds you about a month before expiry.
Time to complete	You have **six months** from application to submit before the account closes without refund. If you fail, you get the assessor's comments and **two working days** to fix and resubmit free of charge. Realistically: one to three weeks of elapsed time for a prepared micro business.
Free preparation	IASME's Cyber Essentials Readiness Tool (getreadyforcyberessentials.iasme.co.uk) produces a tailored action plan. The NCSC Cyber Action Toolkit (cybertoolkit.service.ncsc.gov.uk) is broader and not scheme-specific.

Get the scope right before you answer anything

Scope is where micro businesses fail. Three rules decide almost everything:

- **Cloud services cannot be excluded.** Version 3.3 says so explicitly and defines a cloud service as an on-demand, scalable service on shared infrastructure, accessed via an account and storing or processing your data. **Every** such service must be listed: AWS, Laravel Forge, GitHub, Twilio, OpenAI, Mux, Pusher, your email provider, your monitoring tools, your password manager, your accounting software, and even your social media accounts, which the question set names as cloud services.
- **You are always responsible, even where the provider implements the control.** Your EC2 instances are Infrastructure as a Service, which the requirements document names AWS EC2 as an example of, so operating system patching, firewall configuration, secure configuration and malware protection on those instances are yours. **User access control is yours for every cloud service type**, without exception. Where a provider implements a control for you, you must be able to point to a contract term, security statement or privacy statement that commits them to it.
- **End-user devices are in scope and cannot be left out.** "A scope that doesn't include end-user devices isn't acceptable." Company laptops and any personal device used for company work are in scope. Devices used *only* for native voice, native text or a multi-factor authentication app are out. Devices owned by a third party, such as a contractor's own laptop, are out, but any account you own is in scope even when a contractor uses it.
- **Home routers are out unless you supplied them.** "If your organisation gives the home or remote worker a router, that router is then also in scope. All other routers are out of scope", which means you must apply the firewall controls through a **software firewall on the device instead**. Do not describe a home router in the assessment.

- **Your own application code is out of scope.** "Bespoke and custom components of web applications are out of scope." The TeamTalk Laravel application you wrote is not assessed. Everything it runs on is: the operating system, PHP, nginx, MySQL, Redis and every third-party Composer and npm package, all of which must be supported and patched.

Aim for **whole organisation** certification. A "partial organisation" scope is allowed but it is what a procurement reviewer will notice and ask about, and it undoes most of the value of holding the certificate.

The five controls, mapped to this stack

1 Firewalls

- [ ] AWS security groups deny inbound by default. Only 443 is open to the world; SSH is restricted to a named source address range or is closed. **Every inbound rule is documented with the business need and approved by a named person.**
- [ ] Rules that are no longer needed are removed, and the rule set is reviewed [quarterly].
- [ ] The host firewall on each server (ufw, managed by Laravel Forge) is enabled and matches the security group.
- [ ] MySQL and Redis are not reachable from the internet. Databases sit in a private subnet or are bound to localhost.
- [ ] No administrative interface is reachable from the internet without either multi-factor authentication or an IP allow list combined with a properly managed password. That includes the Forge dashboard, the AWS console, phpMyAdmin if present, and any admin panel.
- [ ] Default administrative passwords on any firewall or router are changed to a strong unique password, or remote administration is disabled entirely.
- [ ] **Software firewall enabled on every laptop**, because home routers are out of scope and the device firewall is what replaces them.

EVIDENCE TO KEEP · a dated export or screenshot of the AWS security group rules with a one-line business justification per rule; the output of `ufw status verbose`; a screenshot of the firewall setting on each laptop; the name of the person who approves rule changes.

2 Secure configuration

- [ ] Unnecessary user accounts are removed or disabled on servers and in every cloud service. Guest accounts and unused administrative accounts are gone.
- [ ] **No default or guessable passwords anywhere.** Check the database root account, any seeded application admin account, and every appliance.
- [ ] Unnecessary software and services are removed or disabled: sample applications, unused PHP extensions, unused system daemons, default web server pages.
- [ ] Auto-run is disabled so files cannot execute without user authorisation.
- [ ] Users are authenticated before they reach any organisational data or service. There is no unauthenticated route into a tenant.
- [ ] Device locking is configured on every laptop and phone: automatic lock after a short idle period, and a credential to unlock. **A device-unlock credential must be at least 6 characters**; if the same credential authenticates anywhere else, the full password rules in control 4 apply.
- [ ] Cloud services are reviewed and any feature not needed for day-to-day use is switched off.

EVIDENCE TO KEEP · a build or provisioning note for the server describing what is installed and why; a list of accounts on each server and cloud service with a last-reviewed date; laptop screen-lock settings.

3 Security update management TWO AUTO-FAIL QUESTIONS

- [ ] **All software is licensed and supported.** No end-of-life PHP branch, no unsupported Ubuntu release, no abandoned Composer or npm package with no vendor support. Unsupported software must be removed, upgraded, or isolated in a sub-set with no internet access.
- [ ] **Updates that the vendor rates critical or high, or that carry a CVSS v3 base score of 7 or above, or where the vendor gives no severity, are installed within 14 days of release.** This is the hard requirement and it applies to servers, laptops, phones, routers and firewalls. Answering "no" to either the operating system question or the applications question is an automatic fail.
- [ ] Automatic updates are enabled wherever possible: unattended-upgrades on Ubuntu, automatic updates on macOS and Windows, automatic browser updates.
- [ ] A named person checks Composer and npm advisories on a [monthly] cycle and after any security announcement, with automated dependency alerting switched on in the repository.
- [ ] There is a written note of the process, because the assessor asks how you know within 14 days, not merely whether you patch.

EVIDENCE TO KEEP · the unattended-upgrades configuration and its log; a dated list of operating system versions and their end-of-support dates; dependency alert history; the date and version of the last framework and PHP upgrade.

4 User access control FOUR AUTO-FAIL QUESTIONS

This is the control that changed in April 2026 and the one most likely to fail a micro business. Multi-factor authentication on cloud services is now mandatory and is assessed as an automatic fail, whether the provider offers it free, bundled or as a paid option.

- [ ] **MFA is enabled on every cloud service account, for every user and every administrator.** Go through the list one by one: AWS root and IAM, Laravel Forge, GitHub, Twilio, OpenAI, Mux, Pusher, the email provider, monitoring, the password manager, accounting, and social media accounts. If a service offers MFA and you have not enabled it, that alone fails the assessment.
- [ ] Where a service genuinely offers no MFA, it is listed in the answer to the relevant question. If the assessor finds MFA was in fact available, that is an automatic fail.
- [ ] The password paired with MFA is at least 8 characters, with no maximum length limit.
- [ ] Password quality is managed by **one** of: MFA; a minimum of 12 characters; or a minimum of 8 characters together with automatic blocking of common passwords from a deny list. Passwordless authentication, including FIDO2 passkeys, is accepted and counts as MFA.
- [ ] Brute-force protection is in place: throttling to no more than 10 guesses in 5 minutes, or device lockout after no more than 10 failed attempts, or MFA.
- [ ] **Password expiry is not enforced, and complexity rules are not enforced.** The scheme requires you not to do these; an old policy that forces a 90-day change is now a non-conformance.
- [ ] **Separate administrative accounts.** Administration is done from an account used only for administration. Day-to-day email and web browsing never happen from an administrative account, on the server, in AWS or in any cloud service. Downloads are made as a standard user and installed as an administrator.
- [ ] There is a written approval process for creating an account and for granting administrative rights, a tracked list of who holds administrative accounts, and a documented review of that list [quarterly].
- [ ] Accounts are removed on a person's last working day, including SSH keys, cloud service accounts and shared password manager access.

EVIDENCE TO KEEP · a single spreadsheet listing every cloud service, its account holders, whether each is an administrator, and whether MFA is on, with a date; the account approval note; the access review record; a screenshot of the AWS IAM credential report.

5 Malware protection

- [ ] Each in-scope device uses **one** of: anti-malware software, or application allow-listing restricted by code signing.
- [ ] Where anti-malware software is used it updates in line with the vendor's instructions, prevents malware from running, prevents malicious code executing, and prevents connections to known malicious websites. The protection built into macOS and Windows is acceptable, provided it is switched on and updating.
- [ ] **The "Applies to" line includes servers.** Decide and record your approach for the Ubuntu EC2 instances rather than leaving the question blank: either anti-malware, or an allow-listing argument you can defend to the assessor.

EVIDENCE TO KEEP · a screenshot per laptop showing protection enabled and definitions current; a written note of the server approach and the reasoning.

Not a requirement, but say it anyway

Backups are not a technical requirement of Cyber Essentials. The v3.3 requirements say so explicitly while strongly recommending them, and version 3.3 added emphasis on backing up. Answer the backup question fully anyway: it costs nothing and the same answer feeds straight into the supplier questionnaire, which does treat backup and restore as a scored item.

How to answer the self-assessment

- **Download the Danzell question set first and answer it in a document before you pay.** IASME publishes it free. Working through it offline shows you the gaps while you can still fix them, and the six-month clock has not started.
- **Answer the question that was asked.** Assessors mark against the requirements document, not against a general impression of your security. "We take security seriously" scores nothing. "Unattended-upgrades is enabled on all three servers; critical and high severity updates are applied within 14 days; the last manual check was on [date]" scores.
- **Never claim a control you have not implemented.** A wrong answer that is discovered is worse than a "no" that comes with a remediation date, and the two-working-day resubmission window exists precisely so that a "no" can be fixed.
- **Name real things.** Actual server names, actual service names, actual dates. Vague answers get queried, and every query adds days.
- **A board-level declaration is required.** The signatory confirms the answers are true and acknowledges an ongoing responsibility for compliance, not just compliance on the day.
- **Certification is a point in time**, being the date the certificate is issued. Nothing stops you changing the estate afterwards, but you re-answer everything at renewal, so it is cheaper to keep the controls in place than to rebuild the evidence each year.

Before you apply: the ten-minute pre-flight

	CHECK	WHY IT MATTERS
☐	Every cloud service listed, with MFA on	Four automatic fails live here
☐	No unsupported software anywhere in scope	An automatic certification blocker
☐	14-day patching demonstrable, not just claimed	Two automatic fails
☐	Separate administrative accounts, not one account doing both jobs	The most common micro-business finding
☐	Password expiry switched off	An old habit that is now a non-conformance
☐	Laptop software firewalls on, home routers not mentioned	Scope error that triggers assessor questions
☐	Whole organisation scope, not partial	Partial scope invites procurement questions
☐	Named signatory ready for the board declaration	Submission cannot complete without it

Sources, verified 28 August 2026: NCSC, Cyber Essentials overview and the five controls ncsc.gov.uk/cyberessentials/overview; NCSC, *Cyber Essentials: Requirements for IT Infrastructure v3.3*, April 2026, effective 27 April 2026 ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf; IASME, Danzell question set version 16.3, May 2026 iasme.co.uk preview the self-assessment questions; IASME, Cyber Essentials pricing and frequently asked questions iasme.co.uk/cyber-essentials; IASME, changes to Cyber Essentials for April 2026 iasme.co.uk/articles; IASME Readiness Tool getreadyforcyberessentials.iasme.co.uk; NCSC Cyber Action Toolkit cybertoolkit.service.ncsc.gov.uk.