

Cyber Essentials readiness checklist

A free 15-minute self-check for small teams, from TekSupport.co.uk

TekSupport.co.uk will help you get Cyber Essentials certified. We prepare you for the five controls and help you submit.

A licensed Certification Body, working through IASME, marks the assessment and issues the certificate. Our £295+VAT visit is a paid gap list. The IASME fee is separate, and we can't guarantee a pass.

How to use this checklist

Cyber Essentials is the UK Government-backed baseline for cyber security. It has five technical controls that protect against the most common internet attacks. You answer an online self-assessment questionnaire, a senior person in your organisation signs to confirm the answers are true, and an assessor marks it.

Go through each line below and tick **Yes**, **No** or **Not sure**. Every **No** or **Not sure** goes on your to-do list. Be honest: the real assessment asks for detail, and a wrong answer only delays you.

Which question set applies to you?

- If you buy your assessment **from 27 April 2026**, you'll answer the **Danzell** question set, which is based on the NCSC's Requirements v3.3. This checklist follows Danzell.
- If you bought **before 27 April 2026**, your account uses the previous **Willow** set. IASME gives you six months from applying to complete and submit, so check your account date.

The  symbol marks items that are an **automatic fail** under Danzell.

Step 0: Scope. What's in and what's out?

Get this right first. Most surprises come from things people forgot were in scope.

☐ Check

- ☐ We've decided whether we're certifying the **whole organisation** or a clearly separated part of it (a "sub-set" split off by a firewall or VLAN). The whole organisation gives the best protection, and a partial scope has to be justified to the assessor.
- ☐ We have a list of every **laptop, desktop, tablet and phone** used for work, including their operating system and version. A scope with no end-user devices isn't acceptable.
- ☐ We've included **personal devices (BYOD)** that access work email, files or apps. Phones used only for calls, texts or an MFA app are out of scope.

☐ Check

- ☐ We've included **home and remote workers' devices**. If we gave someone a router, that router is in scope too.
- ☐ We've listed every **server** (physical, virtual or cloud-hosted).
- ☐ We've listed every **firewall and router**, including the office broadband router.
- ☐ We've listed **every cloud service** that holds or processes our data: Microsoft 365 or Google Workspace, accounting, CRM, file sharing, HR, booking systems, and business social media accounts. **Cloud services can't be left out of scope.**
- ☐ We know which accounts are used by **outside suppliers or IT providers** to manage our systems. Those accounts are in scope too.
- ☐ Devices we lend to volunteers, trustees or contractors are included.

Control 1: Firewalls

Aim: only safe, necessary services can be reached from the internet.

☐ Check

- ☐ Every in-scope device is protected by a firewall: the office boundary firewall or router, and/or the **software firewall built into Windows or macOS**, switched on.
- ☐ Laptops used at home, on public Wi-Fi or on the move have their **software firewall switched on**.
- ☐ The **default admin password** on every router and firewall has been changed to a strong, unique one, or remote admin is switched off.
- ☐ The router or firewall **admin page can't be reached from the internet**. If it must be, there's a documented business reason and it's protected by MFA or an IP allow list.
- ☐ **Unauthenticated inbound connections are blocked** by default.
- ☐ Every inbound rule, such as a port forward, has been **approved and documented** by an authorised person, with the business reason written down.
- ☐ Rules that are **no longer needed have been removed**. We've reviewed our firewall rules in the last 12 months.

Control 2: Secure configuration

Aim: devices are set up securely and only run what they need.

☐ Check

- ☐ **Unused accounts are removed or disabled**, including guest accounts and admin accounts no one uses.
- ☐ **Default or guessable passwords are changed** on all devices and software.
- ☐ **Software nobody needs has been removed**, including apps, utilities and network services.
- ☐ **Auto-run is switched off**, so files and USB sticks can't run anything without the user's say-so.
- ☐ Users must **sign in before accessing** any work data or services.
- ☐ Every device has a **screen lock**: a password, PIN or biometric. A PIN or password used only to unlock the device is at least **6 characters**.
- ☐ Devices **lock or slow down after repeated wrong guesses**: no more than 10 attempts, or no more than 10 guesses in 5 minutes. Where you can't configure this, the vendor's default is used.

Control 3: Security update management

Aim: devices and software aren't open to known security holes that already have fixes.

☐ Check

- ☐ All software on in-scope devices is **licensed and still supported** by the vendor. **Unsupported software in scope means a fail** (for example, an old Windows version, or an app or router with no more security updates). Remove it, or move it into a separate network with no internet access.
- ☐ **Automatic updates are switched on** wherever possible.
- ☐  **High-risk or critical updates for operating systems and router/firewall firmware are installed within 14 days** of release. (Danzell A6.4, an automatic fail.)
- ☐  **High-risk or critical updates for applications, including their extensions and associated files, are installed within 14 days** of release. (Danzell A6.5, an automatic fail.)
- ☐ We treat an update as high-risk if the vendor calls it critical or high risk, if it fixes a vulnerability scored **CVSS 7 or above**, or if the vendor gives **no details** of what it fixes.
- ☐ We can show dates: when an update came out and when it was installed.

Good practice (not required): install all updates within 14 days, not just the critical ones.

Control 4: User access control

Aim: accounts belong only to the right people and only have the access they need.

☐ Check

- ☐ There's a **process to create and approve** new user accounts.
- ☐ Everyone has **their own login**. No shared accounts for day-to-day work.
- ☐ **Leavers' accounts are removed or disabled** promptly, and inactive accounts after a set period.
- ☐ Staff who need admin rights have a **separate admin account**, used only for admin tasks. No email or web browsing on it.
- ☐ **Admin rights are removed** when someone changes role and no longer needs them.
- ☐  **MFA is switched on for every administrator** of every cloud service that offers it. (Danzell, an automatic fail.)
- ☐  **MFA is switched on for every user** of every cloud service that offers it, whether MFA is free, included or a paid add-on. (Danzell, an automatic fail.)
- ☐ We've listed any cloud services that **don't offer MFA at all**. The assessor will check that they really don't.
- ☐ Password-only logins are protected against guessing by **MFA, throttling or lockout** after no more than 10 attempts.
- ☐ Passwords are long enough: **at least 12 characters**, or **at least 8 characters with a block on common passwords**, or protected by MFA. No maximum length. (Where MFA is used, the password part is at least 8 characters.)
- ☐ We **don't force regular password changes** or complexity rules. We **encourage three random words** and a **password manager** instead.
- ☐ We have a quick process to **change passwords** when an account may be compromised.

Passwordless sign-in, such as passkeys, FIDO2 security keys or biometrics, is recognised under v3.3.

Control 5: Malware protection

Aim: stop known malware and untrusted software from running.

☐ Check

- ☐ **Every in-scope device** has active malware protection.

☐ Check

- ☐ On Windows and Mac devices using **anti-malware software** (such as the built-in Microsoft Defender), it's **kept up to date**, **blocks malware from running** and **blocks connections to malicious websites**.
- ☐ Or, where used, **application allow listing** means only approved, code-signed apps can run, there's a current list of approved apps, and users can't install unsigned apps.
- ☐ Phones and tablets only install apps from the **official app store**, and the store's protection is left on.

Not required, but strongly recommended: backups

Backups aren't one of the five controls, but the NCSC's v3.3 Requirements specifically recommend them.

☐ Check

- ☐ Important data is backed up automatically, to cloud storage or another device.
- ☐ Any USB or external backup drive is **disconnected** when a backup isn't running.
- ☐ We've actually **tested a restore** recently.

Your score

- **All Yes:** you're in good shape. Download the free question set from IASME and draft your answers.
- **Any ⚠ item is No or Not sure:** fix these first. Under Danzell they fail the whole assessment.
- **A few No or Not sure answers elsewhere:** usually quick to fix, but each one needs sorting before you apply.

What happens next

1. **Read the questions for free.** IASME publishes the full Danzell question set (PDF and Excel) so you can prepare your answers before paying. IASME also has a free **Cyber Essentials Readiness Tool**.
2. **Buy the assessment.** The IASME fee depends on headcount: **£320 + VAT** for 0 to 9 staff, **£440 + VAT** for 10 to 49, **£500 + VAT** for 50 to 249 and **£600 + VAT** for 250 or more (IASME FAQ, checked 26 Sep 2026). This fee is separate from anything you pay us.
3. **Complete and submit.** You have six months from applying. A board-level or senior person signs a declaration that the answers are true.
4. **Assessment.** A licensed Certification Body marks it. IASME says most assessors aim to return results within about 3 days. If something isn't compliant, you normally get 2 working days to

fix it and resubmit without paying again.

5. **Renew every year.** Certificates last 12 months.

How TekSupport.co.uk can help

TekSupport.co.uk will help you get Cyber Essentials certified. We prepare you for the five controls and help you submit.

- **£295 + VAT on-site visit:** we map your scope (laptops, phones, home workers, routers and every cloud service) and walk the five controls with you. You leave with a **written gap list** of what would fail today, including the automatic fails.
- **Help submitting:** we can help you complete and submit the IASME questionnaire. A senior person in your organisation still confirms the answers.
- **Monthly checks (optional, part of our monthly IT desk):** each month we check that MFA is still on, critical updates are inside 14 days, leavers are gone, firewall defaults are still changed, malware protection is running and the last backup actually completed.

A licensed Certification Body, working through IASME, marks the assessment and issues the certificate. Our £295+VAT visit is a paid gap list. The IASME fee is separate, and we can't guarantee a pass.

Get in touch: hello@teksupport.co.uk · teksupport.co.uk · Gem Court, 15 Merryweather Place, London SE10 8BZ

This checklist is a free guide to help you prepare. It isn't the official question set and doesn't replace it. The requirements can change each year, so always check the current IASME question set before you apply.

Sources

- NCSC, *Cyber Essentials: Requirements for IT Infrastructure v3.3* (April 2026): [ncsc.gov.uk](https://www.ncsc.gov.uk)
- IASME, *Preview the Self-Assessment questions* (Danzell question set) and *Changes to Cyber Essentials for April 2026*: [iasme.co.uk](https://www.iasme.co.uk)
- IASME, *Cyber Essentials FAQ* (fees and timings, checked September 2026): [iasme.co.uk](https://www.iasme.co.uk)