No Jargon Cyber — Plain-English readiness kits for Cyber Essentials
https://nojargoncyber.co.uk

Cyber Essentials Readiness Checklist 2026

Plain English. Sorted by priority. Up to date for Requirements v3.3 (the "Danzell" question set), which applies to assessments started from 27 April 2026.

Free from No Jargon Cyber — Plain-English readiness kits for Cyber Essentials · Last reviewed November 2026 · https://nojargoncyber.co.uk

> **Independent guidance.** We are not affiliated with the NCSC, IASME or any Certification Body. This checklist does not guarantee certification and is not legal advice. The official documents always take priority: see "Official sources" at the end.

How to use this checklist (15–45 minutes)

1. **Go through it with whoever looks after your IT** (you, a colleague or your IT support company).
2. **Mark each item** ✅ Yes / ❌ No / ❓ Not sure. Count "Not sure" as "No" until you have checked.
3. **Fix the 🔴 Auto-fail items first.** These are the five questions the official Danzell set specifically flags as automatic fails (U3, U4, A1, A2 and A3). One "No" on any of these means you fail, however good everything else is.
4. **Then fix the 🟠 High items.** These are mandatory requirements. Non-compliance fails certification. Start with U1 and U2 (unsupported software): IASME says unsupported software in scope means you will not be certified, even though those questions are not flagged as automatic fails in Danzell.
5. **Then the 🟡 Medium items.** These are required too, but they are usually quick: a written process, a list or a review.
6. **Work out your score** (section 8) and go back over anything that isn't a ✅.

What the priorities mean

Label	Meaning
🔴 **Auto-fail**	A question the official Danzell set specifically flags as an automatic fail (U3, U4, A1, A2 and A3). A "No" here fails the whole assessment. Assessors cannot treat it as a minor issue.
🟠 **High**	A mandatory requirement. Non-compliance fails certification. If you can't honestly answer yes, you are not ready to apply.
🟡 **Medium**	Still a requirement, usually about having a process or record. Often fixed in an afternoon.
🟢 **Recommended**	Not required for Cyber Essentials, but strongly advised by the NCSC.

Five Danzell questions are officially automatic-fail questions (A6.4, A6.5, A7.15, A7.16, A7.17). Unsupported software isn't labelled that way, but it's still mandatory and having it in scope means you fail.

What changed in 2026 (the 60-second version)

- **The standard is now v3.3.** The NCSC's *Requirements for IT Infrastructure v3.3* took effect on **27 April 2026**, alongside IASME's new **"Danzell"** question set. It replaced v3.2 / "Willow".
- **The five controls haven't changed.** What has changed is how strictly some of them are marked.
- **MFA on cloud services is now an automatic fail.** If a cloud service offers multi-factor authentication (free, included or as a paid extra) and you haven't turned it on for every user and every admin, you fail.
- **Late security updates are now an automatic fail.** Critical or high-risk updates for operating systems, router or firewall firmware, and applications must be installed within **14 days** of release.
- **Unsupported software still means you fail certification.** IASME's FAQ is clear that unsupported software in scope stops you getting certified. This is a mandatory requirement, not one of the five Danzell automatic-fail questions. Windows 10 after 14 October 2025 is unsupported unless the device is enrolled in an applicable Microsoft Extended Security Updates (ESU) programme and is receiving the required security updates. Check that programme's eligibility and terms.
- **Cloud services can't be excluded from scope.** v3.3 now defines "cloud service", and it includes free tools staff signed up for with a work email address, as well as social media accounts.
- **Passkeys and FIDO2 security keys count as MFA.**

🚨 The top 10 things that fail people

These are the gaps we see most often in small organisations. Check them before anything else.

1. **One forgotten cloud service without MFA.** It's usually social media, the accounting or payroll app, the domain or web host, or a free tool someone signed up for. Under Danzell, one service is enough to fail you.
2. **An admin account without MFA.** This includes the "spare" global admin, the account your IT company uses, or the original owner account on a SaaS tool.
3. **Windows 10 without an applicable Extended Security Updates (ESU) programme**, or an old Mac or phone that no longer gets updates. Windows 10 after 14 October 2025 is unsupported unless the device is enrolled in an applicable Microsoft ESU programme and is receiving the required security updates. Check that programme's eligibility and terms.
4. **Unsupported apps hiding on laptops.** Examples are old versions of Office, Adobe Reader, Java or PDF tools, abandoned browser extensions and old VPN clients. Extensions and frameworks count.
5. **Updates older than 14 days.** Common causes are a laptop that's been in a drawer, a router whose firmware has never been updated, or a phone stuck on "update later".
6. **The router still has its default admin password**, including the unique one printed on the sticker. Or the admin page can be reached from the internet.
7. **Staff using an admin account every day.** Day-to-day work (email, browsing, invoicing) has to be done from a standard account. Admin rights must be in a separate account.
8. **Shared logins**, such as one "office@" account several people use, or a shared password for the accounting system.
9. **An incomplete scope**: forgetting staff phones that get work email (BYOD), home-working laptops or some of the cloud services.
10. **Leavers who can still log in**, often to a cloud tool that isn't connected to your main Microsoft 365 or Google Workspace account.

---

0. Scope: what you're certifying

Cyber Essentials covers the IT you use to run the business. Get this wrong and every other answer is built on sand.

S1 🟠 You've decided what's in scope and written it down

- **Why it matters:** You have to describe your scope (which part of the business, which networks, which locations), and the assessor has to agree it. Certifying the **whole organisation** is simplest and gives customers the most confidence. Leaving something out needs a justification and a proper network separation.
- **How to check:** Can you write one paragraph saying "This certification covers [whole organisation / named part], at [locations], including home workers, using [networks]"?
- **Evidence tip:** Keep a one-page scope statement. The Accelerator Kit includes a fill-in worksheet.

S2 🟠 You have a list of every device that accesses work data

- **Why it matters:** You'll need to say how many laptops, desktops, servers, tablets and phones you have, with the **make and operating system version**. For Windows, you need the **edition and feature version** (for example "Windows 11 Pro 24H2"). Laptops and phones must be in scope. A scope without end-user devices isn't acceptable.
- **How to check:** Windows: Settings → System → About. Mac: Apple menu → About This Mac. iPhone: Settings → General → About. Android: Settings → About phone.
- **Evidence tip:** A simple spreadsheet with a row per device: owner, make, OS and version, company-owned or personal, last updated.

S3 🟠 You have a complete list of your cloud services

- **Why it matters:** Cloud services **can't be excluded** from scope, and every one of them needs MFA (see A1 to A3). That includes Microsoft 365 or Google Workspace, accounting, CRM, payroll, file sharing, website and domain hosting, **social media accounts**, and free tools staff signed up for with a work email address.
- **How to check:** Look at company card and bank statements for subscriptions. Search the mailbox for "welcome to", "verify your email" and "your account". Ask every member of staff what they log into for work.
- **Evidence tip:** Record service name, what it's used for, admin owner, whether MFA is available and whether it's enforced.

S4 🟠 Staff-owned devices (BYOD) that access work email or files are included

- **Why it matters:** Personal phones and laptops that access organisational data or services are **in scope**. The exception is a device used only for calls, texts or an MFA app.
- **How to check:** Ask: "Does anyone get work email, Teams, Slack or files on a personal phone, tablet or computer?"
- **Evidence tip:** Add them to the device list and mark them "BYOD". Each one has to meet the same rules (supported OS, updates, screen lock and so on).

S5 🟡 You know who's responsible for IT and who'll sign off

- **Why it matters:** You'll name the person who manages your IT, and they **must be a member of your organisation**, not your outsourced IT company. The answers must be approved by a board-level person, owner or equivalent.
- **How to check:** Agree both names now.
- **Evidence tip:** Note both names on your scope statement.

---

1. Firewalls

Goal: only secure, necessary services can be reached from the internet.

F1 🟠 Every office router and firewall has a strong, unique admin password

- **Why it matters:** Default router passwords are published online. The rule applies **even if the router came with a unique password on a sticker**.
- **How to check:** Log in to the router's admin page. If the admin password is still the one on the sticker or in the manual, change it. Use at least 12 characters, or turn on MFA if the router supports it.
- **Evidence tip:** Write down the date you changed it and where the password is stored (for example your password manager), but not the password itself.

F2 🟠 The built-in software firewall is switched on for every computer and server

- **Why it matters:** Home and public networks aren't under your control, so the device's own firewall is its protection. It must stay on **even in the office**, behind a router.
- **How to check:** Windows: Settings → Privacy & security → Windows Security → Firewall & network protection (all profiles on). Mac: System Settings → Network → Firewall (on).
- **Evidence tip:** Take a screenshot per device type, or a report from your device management tool showing the firewall enabled everywhere.

F3 🟠 The router's admin page can't be reached from the internet

- **Why it matters:** An admin login open to the internet is a common way in. It's only allowed if there's a **documented business need** and it's protected by **MFA** or an **IP allow list plus a well-managed password**.
- **How to check:** In the router settings, look for "remote management", "WAN access" or "remote administration". It should be off. If your IT company needs it, ask them to confirm in writing how it's protected.
- **Evidence tip:** A screenshot of the setting, or the IT company's written confirmation and your documented reason.

F4 🟠 Nothing is "opened up" to the internet without approval and a record

- **Why it matters:** Unauthenticated inbound connections must be blocked by default. Any opened port or port forward (for example for remote desktop, a CCTV recorder or a server) needs a business reason, approval from an authorised person and a record.
- **How to check:** In the router, check "port forwarding", "virtual servers", "DMZ" and "UPnP". Remove anything you don't recognise or need. Consider turning UPnP off.
- **Evidence tip:** A short firewall rules log: rule, reason, approved by, date, review date.

F5 🟡 You've reviewed your firewall rules in the last 12 months

- **Why it matters:** Rules that are no longer needed must be removed. You'll be asked how you review them.
- **How to check:** Is there a dated record of the last review?
- **Evidence tip:** Add a "reviewed on / by" line to the rules log and put a yearly reminder in the calendar.

---

2. Secure configuration

Goal: devices and cloud services are set up securely and run only what they need.

C1 🟠 Unused software and services have been removed or disabled

- **Why it matters:** Every unused app is something else to update and attack. This applies to cloud services too: switch off features you don't use.
- **How to check:** Windows: Settings → Apps → Installed apps. Mac: Finder → Applications. Phones: check the home screen and app library. Remove trials, old tools and anything nobody uses.
- **Evidence tip:** Note when you did a clean-up, and keep an approved software list.

C2 🟠 Unused, guest and default accounts are removed or disabled

- **Why it matters:** Forgotten accounts, especially admin ones, are easy targets.
- **How to check:** Windows: Computer Management → Local Users and Groups (or Settings → Accounts → Other users). Mac: System Settings → Users & Groups. Check cloud admin centres for old or test users.
- **Evidence tip:** A dated screenshot or export of user lists after the clean-up.

C3 🟠 Default and guessable passwords have been changed on every device

- **Why it matters:** "admin", "password123" and factory passwords are tried automatically by attackers.
- **How to check:** Check printers, NAS boxes, CCTV, Wi-Fi access points and any shared or kiosk PCs, as well as laptops.
- **Evidence tip:** List the devices checked and the date.

C4 🟠 Auto-run is switched off

- **Why it matters:** Files shouldn't run automatically when a USB stick is inserted or a file is downloaded. Prompting the user to choose what happens is acceptable.
- **How to check:** Windows: Settings → Bluetooth & devices → AutoPlay. Set it off, or to "Ask me every time".
- **Evidence tip:** A screenshot of the setting, or the device management policy.

C5 🟠 Every device locks, and guessing is limited

- **Why it matters:** A device that someone can physically pick up needs a PIN, password or biometric to unlock. Repeated guessing must be limited: **lock after no more than 10 wrong attempts**, or slow attempts down to **no more than 10 guesses in 5 minutes**. Where the vendor doesn't let you configure this, the default is acceptable. A device-only PIN must be **at least 6 characters**.
- **How to check:** Check the screen lock settings on each laptop and phone. Windows: Local Security Policy / device management "account lockout threshold".
- **Evidence tip:** A screenshot of the lock policy, or the MDM / Intune configuration profile.

C6 🟠 Anything you host for remote access requires proper login protection

- **Why it matters:** If you run something people reach over the internet (a VPN, remote desktop, a customer portal, a self-hosted app), users must authenticate. Passwords must be protected by MFA, or by length rules plus throttling or lockout. *(Skip this if you don't host anything. Most small businesses using only SaaS don't.)*
- **How to check:** List anything reachable from outside, then check its login settings.
- **Evidence tip:** A screenshot of the MFA or lockout settings for each external service.

---

3. Security update management

Goal: no known, fixable security holes. **Two of the five automatic-fail items are in this section (U3 and U4).** U1 and U2 are High: they are mandatory, and non-compliance fails certification.

U1 🟠 HIGH (mandatory, non-compliance fails certification): Every operating system is still supported

- **Why it matters:** Unsupported software in scope fails certification. IASME's FAQ is clear on this. This item is marked High, not Auto-fail, because the Danzell question set does not flag it with automatic-fail wording — but a "No" still means you will not be certified. It includes laptops, desktops, servers, phones, tablets, and **router and firewall firmware**. Windows 10 after 14 October 2025 is unsupported unless the device is enrolled in an applicable Microsoft Extended Security Updates (ESU) programme and is receiving the required security updates. Check that programme's eligibility and terms.
- **How to check:** Compare each device's OS version with the vendor's end-of-life page (Microsoft lifecycle, Apple security releases, the Android manufacturer's update policy, the router manufacturer's support page).
- **Evidence tip:** Add a "supported until" column to your device list. Replace, upgrade or retire anything without a future support date.

U2 🟠 HIGH (mandatory, non-compliance fails certification): Every application is still supported, including browser extensions

- **Why it matters:** The same mandatory rule applies to apps, browser extensions, plug-ins, frameworks and runtimes: non-compliance fails certification (IASME FAQ). Software must be supported by a vendor that still produces security fixes. If you genuinely must keep unsupported software, it must be taken out of scope via a defined sub-set that **blocks all internet traffic to and from it**, and that changes your scope.
- **How to check:** Go through installed apps on a few typical devices. Check browser extensions (Chrome or Edge: Extensions page). Look out for old Office versions, old PDF tools, Java, Flash-era tools, discontinued VPN clients and abandoned extensions.
- **Evidence tip:** An approved software list showing the vendor and support status.

U3 🔴 AUTO-FAIL: Critical and high-risk OS and firmware updates are installed within 14 days of release

- **Why it matters:** This now fails automatically. The 14 days run from release. It applies to updates the vendor calls **critical or high risk**, updates fixing vulnerabilities with a **CVSS v3 score of 7 or more**, and updates where the vendor **gives no severity details**. If a bundled update includes even one critical or high fix, the whole update counts.
- **How to check:** Windows: Settings → Windows Update → Update history. Mac: System Settings → General → Software Update. Phones: check for pending updates. Router: check the firmware version against the manufacturer's latest. Look specifically at laptops that are rarely used.
- **Evidence tip:** Screenshots of automatic update settings, plus a weekly patch-check log showing what you checked, what was installed and when. A device management report (Intune, Jamf and so on) is even better.

U4 🔴 AUTO-FAIL: Critical and high-risk application updates are installed within 14 days

- **Why it matters:** The same 14-day rule applies to applications **and their associated files and extensions**: browsers, Office, PDF readers, Zoom and Teams clients, accounting desktop apps, and so on.
- **How to check:** Make sure browsers restart to apply updates. Check that Office is on a supported update channel. Open each key app and look for "Check for updates".
- **Evidence tip:** Note which apps auto-update and how you handle those that don't (for example "checked at least weekly").

U5 🟠 Automatic updates are on wherever possible

- **Why it matters:** This is a requirement in its own right, and it's the easiest way to meet the 14-day rule.

- **How to check:** Check OS auto-update, app store auto-update on phones, browser auto-update and the router's auto-firmware option if it has one.
- **Evidence tip:** Screenshots per device type.

U6 🟠 All software is properly licensed

- **Why it matters:** Software in scope must be both licensed and supported.
- **How to check:** Compare installed paid software against licences and subscriptions.
- **Evidence tip:** A licences tab in your software list.

---

4. User access control

Goal: only the right people get in, with only the access they need. **The other three of the five automatic-fail items are here (A1, A2 and A3).**

A1 🔴 AUTO-FAIL: Every admin on every cloud service uses MFA

- **Why it matters:** Under Danzell, a cloud service administrator without MFA (where the service offers it) fails you automatically. The password part of MFA must be **at least 8 characters**, with no maximum length.
- **How to check:** For each service on your cloud list (S3), open the admin or security settings. Confirm MFA is **enforced**, not just available, for every admin, including spare or emergency admins and accounts your IT provider uses.
- **Evidence tip:** A screenshot of each service's MFA enforcement setting or admin MFA report (for example Microsoft Entra authentication methods report, or Google Admin 2-Step Verification enforcement).

A2 🔴 AUTO-FAIL: Every user on every cloud service uses MFA

- **Why it matters:** The same applies to every standard user. This catches people out on social media accounts, accounting apps and smaller SaaS tools. **Passkeys and FIDO2 security keys count as MFA.** SMS codes count too (though app-based or passkey MFA is recommended). Trusted-location rules on their own don't count.
- **How to check:** Check each service's user list for MFA status. Make sure "legacy" sign-in methods that skip MFA are off.
- **Evidence tip:** An MFA status report or screenshot per service, dated.

A3 🔴 AUTO-FAIL: Any service you think has "no MFA" really has none

- **Why it matters:** You can list cloud services that genuinely offer no MFA. But if you list one that **does** offer it, you fail. If a service can use **sign-in with Microsoft or Google** (single sign-on) to get MFA, you must set that up.

- **How to check:** Search "[service name] two-factor authentication", look in its security settings, and check for "Sign in with Microsoft/Google" options.
- **Evidence tip:** For each "no MFA" service, keep a link or screenshot proving MFA isn't available, and recheck before you submit.

A4 🟠 Everyone has their own login (no shared accounts)

- **Why it matters:** Unique credentials are required for every device, application and cloud service.
- **How to check:** Look for shared mailboxes being logged into directly, shared "admin" logins and generic accounts.
- **Evidence tip:** Convert shared mailboxes into delegated mailboxes and note it in your user list.

A5 🟡 New accounts and admin rights need approval

- **Why it matters:** You need a process for creating and approving accounts, with approval from someone in a leadership role, and a formal process for granting admin access.
- **How to check:** Could you describe it in two sentences?
- **Evidence tip:** A simple starter form or email template: "Please create an account for X, role Y, access Z. Approved by: director."

A6 🟠 Leavers lose access promptly, everywhere

- **Why it matters:** Accounts must be removed or disabled when no longer needed, including after a period of inactivity.
- **How to check:** Compare your current staff list against every cloud service's user list.
- **Evidence tip:** A leaver checklist covering every system on your cloud list, with a date and a signature.

A7 🟠 People only have the access they need

- **Why it matters:** Least privilege applies. When someone changes role, their access should change too.
- **How to check:** Review who can see finance, HR and admin areas.
- **Evidence tip:** Note an annual access review in your user list.

A8 🟠 Admin work uses a separate admin account, and admin accounts aren't used for email or browsing

- **Why it matters:** If someone browsing with admin rights clicks a bad link, the malware gets admin rights too. This applies to **local admin on laptops**, network or domain admin and **cloud admin** accounts. Day-to-day users shouldn't be local admins.
- **How to check:** Windows: Settings → Accounts → Your info (does it say "Administrator"?). Mac: Users & Groups ("Admin"). In Microsoft 365 or Google Workspace, are global admins also

people's everyday mailbox accounts?
- **Evidence tip:** List admin accounts separately from user accounts (for example `admin.jo@`), and write a one-line rule: "Admin accounts are only used for admin tasks."

A9 🟡 You keep a list of who has admin rights and review it

- **Why it matters:** You'll be asked whether you track admin accounts and review them regularly.
- **How to check:** Does the list exist? When was it last checked?
- **Evidence tip:** An admin register with name, systems, approved by, date and last reviewed date.

A10 🟠 Password rules meet the standard

- **Why it matters:** For anything protected by a password, you need one of: **MFA**, **a minimum of 12 characters**, or **a minimum of 8 characters plus automatic blocking of common passwords**, with no maximum length in all cases. Brute-force protection is required (MFA, throttling or lockout after 10 attempts). Don't force regular password expiry or complexity rules.
- **How to check:** Check the password policy in Microsoft 365 / Entra, Google Workspace and any local systems.
- **Evidence tip:** A screenshot of each password policy.

A11 🟡 Staff know how to choose good passwords, and you know what to do if one leaks

- **Why it matters:** You must help people choose unique passwords (for example **three random words** and a **password manager**) and have a process to change passwords promptly if an account may be compromised.
- **How to check:** Is there a short written guide and a short "what to do if" procedure?
- **Evidence tip:** A one-page password and MFA policy that staff have read (the Accelerator Kit includes one).

---

5. Malware protection

Goal: stop malware being delivered and stop it running.

M1 🟠 Every Windows and Mac device has active, updating anti-malware

- **Why it matters:** Each device needs at least one protection option. For Windows and macOS this is usually anti-malware. It must update in line with the vendor's guidance, stop malware running and stop malicious code running. **Microsoft Defender is acceptable.**
- **How to check:** Windows: Windows Security → Virus & threat protection (real-time protection on, definitions up to date). Mac: check your chosen product's status.
- **Evidence tip:** A screenshot per device type, or a central console report.

M2 🟠 Malicious websites are blocked

- **Why it matters:** Anti-malware must also prevent connections to malicious websites. Microsoft Defender SmartScreen can do this on Windows 11.
- **How to check:** Windows Security → App & browser control → Reputation-based protection (on). Check that the browser's safe-browsing protection is on.
- **Evidence tip:** A screenshot of the setting.

M3 🟠 Phones and tablets only install approved apps from official stores

- **Why it matters:** For phones and tablets, protection usually comes from **application allow listing**: apps only from the official store, no unsigned apps, and a list of apps your organisation has approved. This applies to **personal devices used for work** too. You don't need device management software if policy, process and training do the job.
- **How to check:** No jailbroken or rooted devices. Is there an approved app list?
- **Evidence tip:** An approved apps list plus the BYOD policy that staff have signed.

---

6. Recommended extras (not required, but strongly advised)

R1 🟢 Automatic backups are on, and one copy is kept offline or separate

- **Why it matters:** The NCSC highly recommends backups in v3.3, even though they're not a requirement. Backups are what get you through ransomware. If you use a USB drive, disconnect it when it isn't backing up.

R2 🟢 You've signed up to the NCSC's free Early Warning service

- **Why it matters:** It's free and alerts you to possible attacks on your network. The application form asks whether you've signed up.

---

7. Before you pay for the assessment

- [ ] You've downloaded the **free official question set** and the **Requirements v3.3** document (links below) and read them through.
- [ ] Every 🔴 and 🟠 item above is ✅.
- [ ] You've drafted your answers in a document first, not straight into the portal.
- [ ] Your board-level sign-off person has read and agreed the answers.
- [ ] You know the price: from **£320 + VAT** for micro organisations (0–9 staff) via IASME. **Check the government's First Step Fund:** 75% off (so £80 / £110 / £125 + VAT) for micro, small and medium-sized organisations (up to 249 staff) that are **registered in the UK**, have **not held Cyber**

Essentials in the last four years, and are within the **Minimal Financial Assistance** subsidy-control limit of **£315,000** under the Subsidy Control Act 2022 (including this discount). You must **register and purchase by 31 March 2027**, or until funding runs out, and then you have six months to submit. IASME's Supplier Assurance Tool checks eligibility. Apply at firststep.iasme.co.uk.

- [ ] You've blocked out time to respond: if you fail, IASME gives you **2 working days** to fix issues and resubmit at no extra cost.

---

8. Scoring your readiness

Score each item you answered ✅ **Yes**. "No" and "Not sure" score 0.

Priority	Points per ✅	Items	Maximum
🔴 Auto-fail	10	5 (U3, U4, A1–A3)	50
🟠 High (U1, U2 — mandatory, non-compliance fails)	10	2	20
🟠 High	5	24 (S1–S4, F1–F4, C1–C6, U5–U6, A4, A6, A7, A8, A10, M1–M3)	120
🟡 Medium	2	5 (S5, F5, A5, A9, A11)	10
Total		**36**	**200**

If C6 doesn't apply to you (you don't host anything people reach over the internet), score it as ✅. Recommended items (R1, R2) aren't scored. High items total 26 (U1, U2 plus the 24 others) for 140 points.

Your readiness % = your points ÷ 200 × 100 (so your points ÷ 2)

What your result means

The percentage bands and time estimates below are **No Jargon Cyber's own planning guide**. They are not official NCSC or IASME scoring, pass thresholds or completion guarantees. **A high percentage cannot make up for a missing requirement.**

Rule 1: any 🔴 item not ✅ means "Not ready", whatever your percentage. U1 and U2 are High, not Auto-fail, but unsupported software in scope also fails certification (IASME FAQ). If either is not ✅, treat your result as "Not ready" as well.

Result	What it means	What to do next
Not ready: auto-fail risk (any 🔴 not ✅)	You would fail today, even with a high score elsewhere.	Fix the red items first. MFA usually takes a day.
Not ready: unsupported software (U1 or U2 not ✅)	IASME says unsupported software in scope fails certification, even though this is not a Danzell automatic-fail question.	Upgrade, replace or retire unsupported systems, or enrol eligible Windows 10 devices in an applicable ESU programme and confirm they are receiving the updates.
Below 70%	Several core controls are missing.	As a planning guide, expect 2–6 weeks of part-time work. Go control by control.
70–89%	You're close. The gaps are usually admin accounts, processes and documentation.	As a planning guide, expect 1–2 weeks. Write up your processes and collect your evidence.
90–100% with all 🔴 items and U1–U2 ✅	You're likely ready to draft your answers — provided no mandatory requirement is still outstanding.	Draft your answers offline, get sign-off, then apply.

Official sources (always check these)

- NCSC – Cyber Essentials help and resources (requirements, question set, Readiness Tool): https://www.ncsc.gov.uk/cyberessentials/resources
- NCSC – *Cyber Essentials: Requirements for IT Infrastructure v3.3*: https://www.ncsc.gov.uk/files/cyber-essentials-requirements-for-it-infrastructure-v3-3.pdf
- IASME – Important update: changes to Cyber Essentials for April 2026: https://iasme.co.uk/articles/important-update-changes-to-cyber-essentials-for-april-2026/
- IASME – Cyber Essentials FAQ (prices, timings): https://iasme.co.uk/cyber-essentials/frequently-asked-questions/
- IASME – First Step Fund (75% off, register and purchase by 31 March 2027, or until funding runs out): https://firststep.iasme.co.uk/
- GOV.UK – Cyber Essentials funding package (First Step Fund): https://www.gov.uk/government/publications/cyber-essentials-funding-package/cyber-essentials-funding-package

---

Want the whole thing done for you?

The **No Jargon Cyber Cyber Essentials Accelerator Kit** turns this checklist into a finished submission pack:

- step-by-step guides for each control
- a scope worksheet and device/software inventory
- six ready-to-edit policies
- evidence worksheets
- a question-by-question prep workbook
- an AI prompt pack

→ https://nojargoncyber.co.uk/kit

No Jargon Cyber is independent and not affiliated with, approved by or endorsed by the NCSC, IASME or any Certification Body. We do not use official logos. Using this checklist does not certify you and does not guarantee certification. General guidance only, not legal or professional advice. © 2026 No Jargon Cyber. You may share this checklist unchanged with attribution.

No Jargon Cyber is independent and not affiliated with, approved by or endorsed by the NCSC, IASME or any Cyber Essentials Certification Body. We don't use official logos or certification marks. We use the name "Cyber Essentials" only to describe the scheme our materials help you prepare for. Our tools and kits do not certify you, do not guarantee certification, and are not legal advice. Questions: hello@nojargoncyber.co.uk.