SNO
A smarter tomorrow.

PRACTICAL CHECKLIST

Cyber Essentials & Cyber Essentials Plus Readiness Checklist

A practical self-assessment against the NCSC's *Cyber Essentials: Requirements for IT Infrastructure* v3.3 (the "Danzell" question set, in effect from 27 April 2026). Find your gaps before your assessor does.

Scope | Firewalls | Secure configuration | Security updates | User access & MFA | Malware protection | CE+ preparation

How to use this checklist

Cyber Essentials is the UK government-backed scheme, run by the NCSC with IASME as delivery partner, that helps organisations guard against the most common cyber attacks. It covers five technical controls. Cyber Essentials Plus adds independent technical testing of the same controls.

Work through it in order

- Start with **Scope**. Everything else depends on it.
- Tick **Yes** only if you could show evidence today.
- Treat **Partly** and **No / not sure** as actions.
- Fix anything marked AUTOMATIC FAIL first.

Who should complete it

- Your IT lead or managed service provider, with
- someone who knows your cloud subscriptions and starters and leavers (often finance or HR), and
- the director who will sign the declaration.

What changed in 2026

- **Automatic fails:** not using MFA on a cloud service where it's available, and not installing critical or high-risk updates within 14 days (questions A6.4 and A6.5).
- **Cloud services can't be excluded** from scope, and "cloud service" is now formally defined.
- **Scope is stricter:** "untrusted" and "user-initiated" no longer qualify internet connections. You must describe and justify exclusions and list every legal entity in scope.
- **"Point in time" is the certificate date.** The director's declaration now covers compliance for the whole certification period.
- **Cyber Essentials Plus:** if the first sample fails on updates, you must fix the whole scope and a new sample is tested too. A second failure revokes the CE certificate. Self-assessment answers can't be changed once CE+ testing starts.
- **FIDO2 passkeys** are now named as passwordless authentication and regarded as MFA.

Important

This checklist is a preparation aid, not an official question set, and it doesn't guarantee certification. Certification can only be awarded by an IASME-licensed Certification Body against the current requirements. Always check the latest NCSC and IASME documents (see References) and your Certification Body's guidance. Requirements are reviewed every year. This edition reflects v3.3 as published in April 2026.

1 Scope: what's in, what's out

Get scope right first. Most delays happen here, and under v3.3 you must now justify every exclusion.

CHECK	YES	PARTLY	NO / NOT SURE
We've listed every legal entity, site and network that will be covered by the certificate, including company names, addresses and company numbers. **CHANGED IN 2026** The 2026 scheme asks you to name every legal entity in scope. Have Companies House details ready.	☐	☐	☐
We've written down anything we're excluding from scope, why, and how it's separated from in-scope systems (for example by a firewall or VLAN). **CHANGED IN 2026** Exclusions must now be described and justified. They aren't shown on your public certificate.	☐	☐	☐
Every cloud service that holds or processes our data is on our list (for example Microsoft 365, Google Workspace, CRM, finance, HR and file-sharing tools). **CHANGED IN 2026** Cloud services can't be excluded from scope. Check finance cards and expense claims for subscriptions IT doesn't know about.	☐	☐	☐
We have an up-to-date asset list of all in-scope devices: servers, desktops, laptops, thin clients, tablets, phones, firewalls and routers. It includes the operating system and version for each. You'll need operating system and version details for the assessment. Out-of-date lists are a common cause of findings.	☐	☐	☐
Staff-owned devices (BYOD) that access work email, files or apps are included. The exceptions are devices used only for calls, texts or an MFA app. BYOD devices that access organisational data or services are in scope.	☐	☐	☐
Home and remote working devices are included. Any router we supply to a home worker is included and managed like an office firewall. Home routers you don't supply are out of scope, so the device's own software firewall must be on.	☐	☐	☐
Accounts used by third parties, such as IT support providers and contractors, are listed and under our control. Third-party accounts are your responsibility under the user access control requirements.	☐	☐	☐

2 Firewalls

Every in-scope device must be protected by a correctly configured firewall, or a network device with firewall functionality.

CHECK	YES	PARTLY	NO / NOT SURE
Every boundary firewall and router has had its default admin password changed to a strong, unique one, or has remote admin access disabled.	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
The admin interface isn't reachable from the internet. Where it must be, the business need is documented and it's protected by MFA, or by an IP allow-list combined with a properly managed password.	☐	☐	☐
Unauthenticated inbound connections are blocked by default.	☐	☐	☐
Every inbound firewall rule has been approved by an authorised person and documented with its business reason. Keep a simple rule register: rule, reason, approver, date.	☐	☐	☐
Rules that are no longer needed are removed or disabled. We review them at least every quarter. A periodic review isn't a stated requirement, but it's the easiest way to show you remove rules when they're no longer needed.	☐	☐	☐
Software firewalls are switched on for laptops and other devices used on untrusted networks such as home or public Wi-Fi. The built-in Windows and macOS firewalls are advised in preference to third-party apps.	☐	☐	☐

3 Secure configuration

Out-of-the-box settings are rarely secure. Remove what you don't need and lock down what you keep.

CHECK	YES	PARTLY	NO / NOT SURE
Unnecessary user accounts (guest accounts and unused admin accounts) are removed or disabled on every device and service.	☐	☐	☐
All default or guessable passwords have been changed. Check printers, network storage, Wi-Fi access points and IP phones as well as computers.	☐	☐	☐
Unnecessary software, utilities and network services have been removed or disabled.	☐	☐	☐
Auto-run is disabled, so files can't run without the user's authorisation, for example when they're downloaded or a USB drive is inserted.	☐	☐	☐
Users must authenticate before they can access organisational data or services.	☐	☐	☐
Devices lock after inactivity and need a PIN, password or biometric to unlock.	☐	☐	☐
Unlock attempts are protected against guessing: no more than 10 attempts in 5 minutes (throttling), or a lock after no more than 10 failed attempts. Where the vendor doesn't allow this to be configured, the vendor default is accepted.	☐	☐	☐
Device-unlock PINs or passwords are at least 6 characters. Where the same credential is also used to sign in, the full password rules in section 5 apply.	☐	☐	☐

4 Security update management

This is where most organisations fail. The 14-day rule is now an automatic fail.

CHECK	YES	PARTLY	NO / NOT SURE
All software on in-scope devices is licensed and still supported by the vendor, with a known end-of-support date. Check operating systems, browsers, plugins, PDF readers, Java, firmware and line-of-business apps.	☐	☐	☐
Unsupported software is removed, or the devices running it are moved out of scope into a separated sub-set.	☐	☐	☐
Automatic updates are enabled wherever possible.	☐	☐	☐
Critical and high-risk updates for operating systems and router or firewall firmware are installed within 14 days of release. **AUTOMATIC FAIL** This applies to updates the vendor rates critical or high risk, with a CVSS v3 score of 7 or above, or with no severity given. Question A6.4.	☐	☐	☐
Critical and high-risk updates for applications, including their associated files and extensions, are installed within 14 days of release. **AUTOMATIC FAIL** Browser extensions and add-ins count. Question A6.5.	☐	☐	☐
We can show evidence of patch status across every in-scope device, not just a sample, for example from an RMM, Intune or patch-management report. This isn't a written requirement, but it's the practical way to prove the 14-day rule across your whole scope.	☐	☐	☐

5 User access control

Control who has accounts, what they can do and how they sign in. The MFA rule is now an automatic fail.

CHECK	YES	PARTLY	NO / NOT SURE
There's a documented process to create and approve user accounts.	☐	☐	☐
Everyone signs in with their own unique credentials. There are no shared logins.	☐	☐	☐
Accounts are removed or disabled promptly when people leave or after a defined period of inactivity. Agree a starters, movers and leavers process with HR.	☐	☐	☐
MFA is enforced on every cloud service where it's available, whether it's free, included or a paid add-on. **AUTOMATIC FAIL** Not using MFA where it's available is an automatic fail. Keep evidence (for example screenshots of Conditional Access or MFA policies) for each service.	☐	☐	☐
MFA is used wherever else it's available, especially for admin accounts and anything accessible from the internet.	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
Admins use a separate account for admin tasks only, with no email, web browsing or other everyday use.	☐	☐	☐
Admin and other special privileges are removed when they're no longer needed, for example when someone changes role.	☐	☐	☐
Password-only sign-ins are protected against guessing by MFA, throttling (no more than 10 guesses in 5 minutes) or a lock after no more than 10 failed attempts.	☐	☐	☐
Password quality is enforced technically by one of: MFA; a minimum of 12 characters; or a minimum of 8 characters with automatic blocking of common passwords. None of these may have a maximum length. Where MFA is used, its password element must be at least 8 characters.	☐	☐	☐
Users are supported to choose good, unique passwords (for example with the three random words approach and a password manager). We don't force regular expiry or complexity rules. These are NCSC-recommended practices.	☐	☐	☐
There's a process to change a password promptly if an account may be compromised.	☐	☐	☐

6 Malware protection

At least one approved mechanism must be active and up to date on every in-scope device.

CHECK	YES	PARTLY	NO / NOT SURE
Every Windows and macOS device (including servers) runs anti-malware that's kept up to date, stops malware running, prevents malicious code executing and blocks connections to malicious websites. Built-in tools such as Microsoft Defender can meet this when correctly configured.	☐	☐	☐
Where we use application allow-listing instead, only approved, code-signed applications can run, we keep the approved list current, and users can't install unsigned software. Allow-listing is an option for all device types, including phones and tablets.	☐	☐	☐

7 Preparing for Cyber Essentials Plus

CE+ tests the same five controls on a sample of your real devices and services. These checks help avoid surprises on the day.

CHECK	YES	PARTLY	NO / NOT SURE
Our verified self-assessment (CE) is completed and certified before CE+ testing starts, and we won't change any answers afterwards. **CHANGED IN 2026** You can no longer adjust the self-assessment based on CE+ results.	☐	☐	☐

CHECK	YES	PARTLY	NO / NOT SURE
We've booked the CE+ audit within the time window our Certification Body allows after the CE certificate (normally 3 months). Confirm the exact window with your Certification Body.	☐	☐	☐
Every in-scope device is fully patched, not just the ones we expect to be sampled. CHANGED IN 2026 If the first random sample fails, you must fix the whole scope and a new random sample is tested as well. A second failure revokes your CE certificate.	☐	☐	☐
The internet-facing IP addresses we'll provide for the external vulnerability scan are correct and complete.	☐	☐	☐
Sample devices can be made available for authenticated internal vulnerability scans: on site, remotely, or via a cloud agent.	☐	☐	☐
Anti-malware or allow-listing will block test files delivered by email and web download on the sampled devices. Run your own harmless test, such as the EICAR test file, first.	☐	☐	☐
MFA is enabled on every in-scope cloud service, and we can demonstrate it to the assessor. AUTOMATIC FAIL	☐	☐	☐
Admin accounts are separate from everyday accounts on the sampled devices and services.	☐	☐	☐

8 Your results and next steps

Number of "No / not sure" answers	
Number of automatic-fail items not yet met	
Target date to resolve all actions	
Planned assessment date	

A practical 30-day plan

- **Week 1:** confirm scope, legal entities and your cloud service list. Close any automatic-fail gaps (MFA, 14-day updates).
- **Week 2:** firewall rule review, removing default passwords and admin account separation.
- **Week 3:** remove unsupported software, confirm malware protection and the device-locking settings.
- **Week 4:** collect evidence, re-run this checklist and book your assessment.

Common reasons for delay

- A cloud app without MFA (often a smaller SaaS tool)
- Unsupported operating systems or firmware still in use
- Browser extensions or plug-ins not patched within 14 days
- An admin using one account for email and admin tasks
- Staff-owned phones accessing email without the required controls

Illustrative examples based on the requirements, not statistics.

Want a second pair of eyes?

SNO helps organisations prepare for Cyber Essentials by making the scope clear, identifying gaps early and supporting remediation before assessment. Start with a Cyber Essentials Readiness Review to get a clear view of your current position and next steps.

Ask an expert: sno.cloud/services/cyber-essentials

01691 888 090 · sales@sno.cloud · www.sno.cloud

References

- NCSC, *Cyber Essentials: Requirements for IT Infrastructure* v3.3 (April 2026): https://www.ncsc.gov.uk/cyberessentials/resources
- IASME, "Important Update: Changes to Cyber Essentials for April 2026" (12 Feb 2026): https://iasme.co.uk/articles/important-update-changes-to-cyber-essentials-for-april-2026/
- NCSC, Cyber Essentials overview: https://www.ncsc.gov.uk/cyberessentials/overview
- NCSC, multi-factor authentication guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
- NCSC, "Three random words": https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

Cyber Essentials requirements © UK Crown Copyright, summarised here for guidance. "Cyber Essentials" is a UK government scheme; SNO is not the scheme owner. © 2026 Specialist Network Operations. Version 1.0, November 2026.