

Cyber Essentials readiness checklist

Work through each item before you apply. Anything you cannot tick is a gap to fix first, because the assessment checks every device and account in scope. These are the gaps we find most often in our own gap analysis.

Scope: know what you are certifying

- ☐ Every laptop, desktop, server, tablet and phone that can reach company data is listed, including staff-owned devices used for work.
- ☐ Every cloud service you use (Microsoft 365, accounts, CRM, file sharing) is listed. Cloud services are always in scope.
- ☐ Routers, firewalls and Wi-Fi access points on your networks are listed, with who manages each one.

1. Firewalls

- ☐ Every internet connection is protected by a firewall, and every laptop has its software firewall switched on.
- ☐ Default admin passwords on routers and firewalls have been changed.
- ☐ Remote admin of the firewall is off, or protected by multi-factor authentication or an IP allow list.
- ☐ Every inbound rule has a documented business reason. Rules nobody needs have been removed.

2. Secure configuration

- ☐ Software, apps and user accounts that are not needed have been removed or disabled.
- ☐ Default and guessable passwords have been changed on every device and application.
- ☐ Auto-run is disabled, so files and USB drives cannot run code without permission.
- ☐ Devices need a PIN, password or biometric to unlock, and lock after repeated wrong attempts.

3. User access control

- ☐ Every person has their own account. There are no shared or generic logins.
- ☐ Admin accounts are separate and only used for admin tasks, never for email or web browsing.
- ☐ Multi-factor authentication is on for every user of every cloud service, starting with admins.
- ☐ Passwords are at least 12 characters, or at least 8 with common passwords blocked automatically.
- ☐ Leavers lose access promptly, and access is reviewed regularly.

4. Malware protection

- ☐ Anti-malware is installed, kept up to date and scanning on every in-scope computer, or only approved applications can run.
- ☐ Phones and tablets only install apps from official app stores.

5. Security update management

- ☐ All software is licensed and still supported. Windows 10 and other unsupported systems are replaced or removed from scope.
- ☐ Automatic updates are on wherever possible.
- ☐ Critical and high-risk updates are installed within 14 days of release, including firmware and third-party apps.

Gaps you cannot close yourself?

PC1 runs a gap analysis, fixes what it finds and submits your assessment through IASME, so you apply once. Guided certification from £1,500 plus the IASME fee. PC1 is Cyber Essentials certified itself.

Call 01792 580 540 or visit pc1.co.uk/cyber-security/cyber-essentials/

Based on the NCSC Cyber Essentials requirements for IT infrastructure. Requirements are updated periodically; check the current version at ncsc.gov.uk before you apply. Updated October 2026.