

Cyber Essentials readiness checklist

Ten questions to check before you apply. Tick each one you can honestly answer yes.



1. SCOPE

Do you have a list of everything that holds or accesses your organisation's data?

Every laptop, desktop, phone, tablet and server, plus every cloud service (email, file storage, accounting, CRM, your domain registrar and so on). Personal devices used for work count too.

If not: You can't protect what you don't know about. Start by listing every device and cloud service, including personal devices used for work email or files.



2. FIREWALLS

Is a firewall switched on for every laptop and desktop, and has the default admin password on your router or firewall been changed?

Your internet router or boundary firewall, and the firewall built into each computer.

If not: Turn on the device firewall everywhere, change default router and firewall passwords, and make sure the admin interface can't be reached from the internet unless it's protected by MFA or an IP allow list.



3. SECURE CONFIGURATION

Have default passwords been changed, and unused accounts and software removed?

Includes printers, routers, Wi-Fi access points and any software you no longer use.

If not: Change every default or guessable password, remove software and accounts you don't need, and turn off auto-run for removable media.



4. DEVICE LOCKING

Do all devices lock automatically and need a PIN, password or biometric to unlock?

Phones and tablets as well as computers, with protection against repeated wrong guesses.

If not: Set every device to lock automatically, require a PIN, password or biometric to unlock, and limit repeated wrong attempts.



5. SUPPORTED SOFTWARE

Is every operating system and application still supported and receiving security updates?

Older versions of Windows, macOS, iOS, Android, Office and other software often fall out of support.

If not: Upgrade or remove anything that no longer gets security updates, or move it out of scope where the scheme allows.



6. SECURITY UPDATES

Are high-risk and critical security updates installed within 14 days of release?

Ideally updates install automatically. Fourteen days is the maximum; we recommend much faster.

If not: Turn on automatic updates where you can, and have a simple process to check that critical and high-risk updates are installed within 14 days.



7. USER ACCOUNTS

Does everyone have their own account, with admin accounts kept separate and used only for admin tasks?

No shared logins, and day-to-day work (email, browsing) done from a standard account.

If not: Give each person their own account, create separate admin accounts for those who need them, and use admin rights only when needed.



8. JOINERS AND LEAVERS

Do you have a process for setting up and removing accounts when people join or leave?

Including access to cloud services and shared mailboxes.

If not: Write down a short process for approving new accounts and removing access promptly when someone leaves or changes role.



9. MULTI-FACTOR AUTHENTICATION

Is MFA turned on for every cloud service that offers it, for every user?

Not just admins and not just Microsoft 365 or Google Workspace: every cloud service that offers MFA.

If not: Turn on MFA for all users on every cloud service that offers it. Partial deployment doesn't meet the requirement.



10. MALWARE PROTECTION

Is anti-malware switched on and up to date on every device, or are only approved applications allowed to run?

Protection built into your operating system counts if it's switched on and updating.

If not: Make sure anti-malware is active and updating on every device, or use application allow-listing so only approved software can run.

What your answers mean

All ten ticked: you may be ready to apply. Our Marking Only service (from £319 + VAT) suits confident teams.

One gap: put it right first, then Marking Only may still suit you. If you would like an assessor alongside you, choose our Supported Service.

Two or more gaps: our Supported Service (from £650 + VAT) gives you your own assessor, who checks every answer before you submit.

Just want to get ready, without certifying yet? Our Readiness Assessment (£350 + VAT, certification not included) checks where you stand.

Take the interactive version, or talk to an assessor: getcybercertified.uk/readiness-check.html