



Cyber Root

Cyber Essentials Readiness Checklist

Aligned to NCSC Requirements for IT Infrastructure **v3.3** (Danzell) · From April 2026

Free from Cyber Root — IASME-licensed Certification Body · Leicester

Tick what you already have. This is a simplified readiness check for SMEs — not a substitute for the official IASME self-assessment. Prioritise items marked **auto-fail**.

Automatic fail under v3.3 / Danzell — fix these first

- MFA not turned on for a cloud service where it is available (free or paid)
- Critical / high-risk security updates not applied within **14 days** of release

0. Scope (start here)

- All cloud services you use are in scope (cloud cannot be excluded under v3.3).
- Work devices are listed (PCs, laptops, servers, tablets, phones used for work).
- Any exclusions are written down, with how they are kept separate from in-scope systems.
- A director or board member will sign the declaration.

1. Firewalls

- A firewall (or router firewall) sits between your network and the internet.
- Default admin passwords on routers/firewalls have been changed.
- Admin pages are not open to the public internet.
- Inbound access is blocked by default; only needed services are allowed.

2. Secure configuration

- Unused accounts are removed or disabled.
- Default passwords on devices and apps have been changed.
- Unnecessary software and services are removed or turned off.
- Devices lock automatically (password, PIN or biometrics).

3. Security update management

- Operating systems and firmware are still supported (not end-of-life).
- Applications in use are supported and licensed.
- Updates are automatic where practical, or someone manages them.
- **Critical / high-risk updates are installed within 14 days** (auto-fail if not).

4. User access control

- Each person has their own account (no shared day-to-day logins).
- Admin accounts are separate and not used for email or browsing.
- Accounts are disabled when people leave.
- **MFA is on for every cloud service that offers it** (auto-fail if missing).
- Passwords meet scheme rules (e.g. 8+ characters with MFA).

5. Malware protection

- Anti-malware is active on work computers (or application allow-listing is used).
- Protection stays up to date and users cannot easily switch it off.

Need help closing the gaps?

Cyber Root is an IASME-licensed Cyber Essentials Certification Body based in Leicester. We help with readiness and certification for Cyber Essentials and Cyber Essentials Plus.

cyberroot.co.uk · info@cyberroot.co.uk · +44 7888 007 527
2-4 Home Farm Square, Leicester, LE4 0RU

Guidance only. Official requirements: NCSC "Cyber Essentials: Requirements for IT Infrastructure" v3.3 and the IASME Danzell question set. Rules at the time of assessment apply. © Cyber Root Ltd · cyberroot.co.uk