UK COMPLIANCE GUIDE FOR IT

Cyber Essentials and Cyber Essentials Plus

Last reviewed: November 2026 · Current version: wise-its.uk/compliance/cyber-essentials/

Please read first. This guide summarises; it is not legal advice. Rules change: check the current version at **wise-its.uk/compliance/cyber-essentials/** and the official sources listed, and ask your legal or compliance adviser to confirm what applies to you.

In brief

Cyber Essentials is the UK government-backed scheme that sets a baseline of technical controls against the most common internet-based attacks. It is run by the National Cyber Security Centre (NCSC), with IASME as the delivery partner that licenses the certification bodies. There are two levels: Cyber Essentials, a self-assessment verified by a certification body, and Cyber Essentials Plus, which adds hands-on technical testing of your systems.

Who it applies to

- Any organisation of any size can certify, and many do so because customers ask for it
- Required for many UK central government contracts that involve handling personal information or providing certain IT services
- Increasingly requested in supply chains, by insurers and in tender questionnaires
- Defence suppliers face additional, separate requirements

What it requires

Firewalls

Every device that connects to the internet is protected by a correctly configured firewall, with default passwords changed and unnecessary services blocked.

Secure configuration

Unused software and accounts removed, default settings changed, and auto-run of unknown software prevented. Devices lock and require authentication.

Security update management

Software is licensed and supported, and high-risk or critical security updates are applied within 14 days of release. Unsupported software is removed or taken out of scope.

User access control

Accounts are created and removed through a process, administrator rights are limited and used only for admin tasks, and multi-factor authentication is used for cloud services where available.

Malware protection

Anti-malware software or application allow-listing protects devices against malicious software.

What it means for your IT

Know what is in scope
Every laptop, desktop, server, phone, tablet, cloud service and network device that accesses organisational data, including staff-owned devices that do.

Remove unsupported software
Old operating systems and applications that no longer receive security updates are the most common reason for failure.

Separate admin accounts
People with administrator rights use a separate account for admin work, never for email or web browsing.

MFA on every cloud service
Including Microsoft 365, line-of-business applications and administrator portals.

Home and mobile working
Devices used away from the office need a software firewall and the same update and malware controls.

Evidence to keep

- A device and software inventory for the whole scope
- Update compliance reports showing timescales
- Multi-factor authentication reports for cloud services
- A list of administrator accounts and who holds them
- Firewall and router configuration records

Common gaps we find

- An unsupported operating system on one forgotten device
- Administrator accounts used for day-to-day work
- A cloud application without multi-factor authentication
- Staff-owned phones accessing email with no management or controls
- Default passwords left on routers or network devices

Key dates

When	What
Every 12 months	Certification is renewed annually to remain current.
Within 3 months	Cyber Essentials Plus testing must be completed within three months of achieving Cyber Essentials.
Periodically, usually April	The requirements and question set are updated. Check the current version before you apply.

Common questions

How long does it take to get certified?
It depends on how many gaps you have. Organisations with supported devices and MFA already in place can prepare quickly; replacing unsupported devices takes longer.

Who signs the application?
A board-level or equivalent person signs the declaration that the answers are true. Your IT provider prepares the evidence, but the declaration is yours.

Does Cyber Essentials make us compliant with UK GDPR?
No. It is good evidence of appropriate technical security, but UK GDPR also covers how you collect, use and keep personal data.

Is insurance included?
Some certifications include cyber liability insurance for eligible small organisations. Check the current terms with the certification body.

Official sources

- National Cyber Security Centre: Cyber Essentials: https://www.ncsc.gov.uk/cyberessentials/overview
- IASME: Cyber Essentials: https://iasme.co.uk/cyber-essentials/

Not sure where you stand?

Take the free cyber maturity self-assessment at **wise-its.uk/resources/cyber-maturity-model**, or ask us for an evidence review at **wise-its.uk/contact**. Wise IT Solutions provides the technical controls, the evidence and the advice; compliance decisions stay with you.

© Wise IT Solutions. Free to share in full with this notice. Last reviewed November 2026.