



CYBER ESSENTIALS · SELF-ASSESSMENT

Are you Cyber Essentials ready? The 25-point checklist

Work through the five controls below and tick, flag or note each line. Every amber or red is simply something to fix before you certify — this is a readiness tool, not a test.

Why this matters: Cyber Essentials is now a gate, not a badge. Under the government's PPN 014 (in force February 2025) it's required for many public-sector contracts, it flows down to subcontractors, and larger clients and insurers increasingly demand it — renewed every 12 months. A tender or renewal is the worst time to discover you're not ready.

GREEN / AMBER / RED

1 Firewalls & internet gateways

☐	1.1 Every device (laptops, servers, firewalls) has a firewall enabled and switched on.	
☐	1.2 Default administrator passwords on routers and firewalls have been changed to something strong and unique.	
☐	1.3 No services or ports are open to the internet unless there is a documented business need.	
☐	1.4 Remote access (RDP, admin panels) is not exposed directly to the internet — it's behind a VPN or private network.	

2 Secure configuration

☐	2.1 Unused software, user accounts and default accounts have been removed or disabled.	
☐	2.2 Auto-run / auto-play is disabled so removable media can't launch software automatically.	
☐	2.3 Devices lock automatically after a short period of inactivity and require a password/PIN/biometric.	
☐	2.4 No shared or generic logins — every person has their own account.	
☐	2.5 Disk encryption (e.g. BitLocker/FileVault) is enabled on laptops and mobile devices.	

3 Security update management

☐	3.1 All operating systems and software still receive security updates from the vendor (nothing end-of-life, e.g. Windows 10 after support ends).	
☐	3.2 Critical and high-severity security updates are applied within 14 days of release — the requirement most firms don't realise they're being measured against.	
☐	3.3 Automatic updates are switched on wherever possible.	
☐	3.4 Someone is actually responsible for checking updates have applied — it isn't left to chance.	

4 User access control

☐	4.1 Every user has their own named account; no accounts are shared between people.	
☐	4.2 Administrator rights are only given to people who genuinely need them, and admins use a separate account for day-to-day work.	

☐	4.3 Multi-factor authentication (MFA) is enabled on email, Microsoft 365 / Google Workspace and other cloud services.	
☐	4.4 Accounts for people who've left are disabled promptly (same day where possible).	
☐	4.5 A password policy is in place — no weak or reused passwords for business systems.	

5 Malware protection

☐	5.1 Anti-malware protection is installed and active on all devices, and kept up to date.	
☐	5.2 Only approved software can be installed — users can't install whatever they like, or you use application allow-listing.	
☐	5.3 Email and web protection is in place to catch malicious attachments and links.	
☐	5.4 Staff have had at least basic guidance on spotting phishing and suspicious messages.	

- **Mostly green?** You're likely close. For many small firms certification is only 2–3 weeks of tidying-up away — worth confirming before your next tender or renewal.
- **A scatter of ambers?** Completely normal, and all fixable. These are the everyday gaps (MFA not everywhere, updates not tracked, old kit lingering) that a short piece of work clears.
- **Several reds?** Don't panic — it just means there's groundwork first. Better to know now than when a contract depends on it.

Want to know exactly where you stand?

Send us this checklist or book a free 20-minute gap call. We'll tell you precisely what stands between you and certification — and quote a fixed price to close the gap. No jargon, no obligation.

smartpathit.co.uk/cyber-essentials →

Smart Path IT — West Yorkshire based, London registered, UK-wide. This checklist is a plain-English readiness aid based on the five Cyber Essentials controls and reflects the current (Danzell) requirements including the 14-day update window. Smart Path IT is Cyber Essentials certified. Certificates are issued by IASME-accredited certification bodies.