YOUR GUIDE TO
Cyber Essentials Certification

What every SME needs to know, do, and fix, including what's changed under the 2026 Danzell update (v3.3).

What Is Cyber Essentials?

Cyber Essentials is the UK Government's flagship cyber security certification scheme, backed by the National Cyber Security Centre (NCSC) and administered by IASME Consortium. It defines a set of five technical controls that, when properly implemented, protect organisations against the most common internet-based attacks, roughly 80% of commodity cyber threats facing UK businesses today.

For SMEs, it serves multiple purposes simultaneously: it reduces real security risk, demonstrates to clients and partners that you take data protection seriously, and is increasingly a mandatory requirement for public sector and government supply chain contracts.

Two tiers of certification:

Cyber Essentials (CE) — A self-assessment questionnaire verified by a certifying body. Suitable for most SMEs as a baseline. Valid for 12 months.
Cyber Essentials Plus (CE+) — The same five controls, but independently verified through hands-on technical testing by an accredited assessor. Required for MOD, NHS and many public sector frameworks.

Why Should an SME Bother?

The honest answer is that Cyber Essentials is one of the most cost-effective things a small business can do for its cyber security posture. Here's why it matters beyond the badge:

- **Contract access:** many public sector, NHS, MOD and local government contracts now require Cyber Essentials as a baseline condition of tendering.
- **Cyber insurance:** insurers increasingly use CE certification as a qualifying criterion or to set premium levels. Uncertified businesses are paying more, or being declined.
- **Supply chain confidence:** larger enterprise clients routinely ask SME suppliers for proof of cyber certification during onboarding and annual reviews.
- **Real risk reduction:** the five controls directly address phishing, ransomware, credential theft, and exploitation of unpatched software, the attacks most likely to affect you.
- **GDPR alignment:** demonstrating technical controls in place is relevant to your obligations under UK GDPR, particularly around data security.

The Five Technical Controls

Every version of Cyber Essentials is built around the same five controls. The Danzell update (v3.3) tightens how rigorously these are assessed, it does not add new controls. Here's what each one requires and what effort looks like for a typical SME:

#	Control	What you must demonstrate	Effort
1	**Firewalls**	Every device connected to the internet must be protected by a properly configured firewall. Rules must be reviewed, documented, and default passwords changed. Personal firewalls required on devices not behind a network boundary.	**Medium**
2	**Secure Configuration**	All devices and software must be configured securely. Remove or disable unused software, services, and default accounts. Apply the principle of least privilege.	**Medium**
3	**User Access Control**	Users must have only the access they need. Admin accounts must be separate from standard accounts. MFA is mandatory on all cloud services and internet-facing systems, under Danzell, missing MFA is an automatic fail.	**Medium**
4	**Malware Protection**	All devices must run active malware protection (anti-malware, application allow-listing, or sandboxing). Signatures/definitions must be kept current.	**Low**
5	**Security Update Management**	All high and critical security updates (CVSS 7.0+) must be applied within 14 days of release across OS, applications, and firmware. Under Danzell, a single unpatched device can fail the entire assessment.	**High**

What's New in 2026: The Danzell Update (v3.3)

The current version of Cyber Essentials is v3.3, using the "Danzell" question set. It became mandatory for all new assessments from 27 April 2026, replacing the previous "Willow" question set (v3.2). If your certificate was issued before that date it remains valid until expiry, but your renewal will be assessed against Danzell.

The Danzell update is the most significant change to the scheme in three years. While the five controls are unchanged, the way they are assessed is stricter, and for the first time the scheme contains automatic-fail questions, meaning certain gaps result in an immediate failure of the entire assessment, with no opportunity to remediate mid-process.

Important:
Danzell introduces automatic-fail questions for the first time in the scheme's history. These are hard gates, your assessor has no discretion to overlook them. Understand them before you submit.

What changed	Detail	Impact
MFA on cloud services — AUTO-FAIL	MFA must be enabled on every cloud service that supports it (Microsoft 365, Google Workspace, Xero, Salesforce, Slack, Dropbox, etc.). If MFA is available, whether free, bundled, or paid, and it is not enabled, the entire assessment fails automatically. No exceptions, no discretion.	**Auto-fail**
Patching — AUTO-FAIL	All high and critical patches (CVSS 7.0+) for operating systems, applications and firmware must be applied within 14 days. Under Danzell (question A6.5), a single unpatched device found during testing fails the entire CE+ assessment. The 14-day rule is unchanged, but enforcement is now absolute.	**Auto-fail**
Cloud services formally in scope	Cloud services now have a formal definition: any on-demand, scalable, internet-accessible service that stores or processes your organisation's data. This means all SaaS, IaaS and PaaS in use (including Microsoft 365, your CRM, accounting software, file storage) must be declared in scope. Cloud services cannot be excluded.	**High**
Simplified scoping	The terms 'untrusted' and 'user-initiated' have been removed as qualifiers for internet connections. Any device connected to the internet that stores or processes organisational data is in scope. This removes ambiguity that some organisations had previously exploited to narrow scope artificially.	**High**
BYOD clarified	Personal devices (phones, laptops, tablets) that access corporate email, cloud services, or data are in scope. They must meet the same technical controls as corporate devices, including MFA, encryption, lock screens, and up-to-date OS. A written BYOD policy alone without enforced controls is insufficient under Danzell.	**High**
Backup guidance added	Backups remain outside the five controls but v3.3 explicitly recommends maintaining them, keeping copies off the primary device, and disconnecting removable media when not in use. CE+ assessors may enquire about resilience posture.	**Medium**
CE+ double sampling	Cyber Essentials Plus introduces a second independent device sample to verify that remediation was applied estate-wide, not just on the initial test devices. Selective patching, fixing only the machines you know will be tested, will now be caught.	**High**
Granular scope questions	The Danzell question set includes new, more detailed questions about scope boundaries, including specific questions about router and application patching (A6.4 and A6.5). Incomplete or vague scope descriptions are more likely to trigger follow-up or failure.	**Medium**
Passwordless authentication	Building on the v3.2 update, v3.3 places further emphasis on FIDO2 authenticators, biometrics, hardware security keys, one-time codes and push notifications as accepted authentication methods alongside traditional MFA.	**Low**

Common Gaps for SMEs, and How to Close Them

Based on assessment patterns, these are the areas where SMEs most frequently fail or require remediation work before they can pass:

1. MFA not enabled on cloud services

The most common failure point, and now an automatic fail under Danzell. Many SMEs have MFA available in their Microsoft 365 or Google Workspace tenancy but have never switched it on, often because it wasn't enforced at setup.

- **Audit every cloud service in use across the business, not just the obvious ones**
- **Enable MFA via Conditional Access in Microsoft 365 (Entra ID) or equivalent in Google Workspace**
- **Don't overlook secondary services: Xero, QuickBooks, your CRM, DocuSign, Dropbox, GitHub**
- **For service accounts and API connections, use app registrations, managed identities or certificates rather than username/password**

2. Unpatched devices and applications

The 14-day patching window is well-known, but enforcement in Danzell is absolute. The gap is usually not patching Windows, it's third-party applications and firmware that auto-updates don't cover.

- **Ensure your patch management tool covers applications (browsers, Office, Adobe, Java), not just the OS**
- **Review router and firewall firmware versions, these are specifically tested in CE+**
- **Document your patching process and be prepared to evidence it, dates applied, CVSS scores tracked**
- **BYOD devices not managed by MDM are particularly high risk here, enforce controls or exclude them from data access**

3. Cloud services not properly scoped

Many SMEs declare a narrow scope, office laptops and a server, without including the cloud services where most of their data actually lives. This is no longer viable under Danzell.

- **Map every service that stores or processes business data, including file shares, email, HR systems, CRM, accounting platforms**
- **All of these must be declared in scope; none can be excluded on the grounds of being 'cloud-hosted'**
- **Ensure MFA is active on all of them before submitting**

4. Firewall rules undocumented or stale

Firewalls are often configured once and never reviewed. CE requires you to be able to demonstrate that rules have been reviewed and that all open ports and services have a documented business justification.

- **Review all inbound and outbound firewall rules in the last 12 months (this is now an explicit question)**
- **Remove or disable rules with no current business purpose**
- **Ensure default admin passwords on routers and firewalls have been changed**
- **Home and remote workers must have personal firewalls active on their devices**

5. Admin account hygiene

Admin accounts used for day-to-day tasks, or shared admin credentials, are common in smaller businesses and will fail the assessment.

- **Ensure every admin account is used only for administration, not for email or general browsing**
- **Remove or disable accounts that are no longer in use, including leavers**
- **MFA must be applied to admin accounts, without exception**
- **Service accounts must be locked down; they should not have interactive login rights unless strictly necessary**

6. BYOD with no enforced controls

Personal devices are in scope if they access business email, Microsoft 365, or any cloud service containing organisational data. A policy document is not sufficient, controls must be technical and enforced.

- **Deploy MDM (Intune, Jamf, or equivalent) or implement conditional access policies that enforce device compliance**
- **As a minimum, require: screen lock with PIN or biometric, device encryption, up-to-date OS, and malware protection**
- **Where enforcing controls on personal devices isn't feasible, consider restricting access to a managed container (e.g. Outlook Mobile with Intune app protection)**

Pre-Assessment Checklist (v3.3 Danzell)

Use this checklist to verify readiness before purchasing your assessment. Address every item, any gap here is likely to result in failure or remediation delay.

Control area	Confirm before submitting
Firewalls	All internet-facing devices are behind a firewall. Firewall rules have been reviewed in the last 12 months. All rules have a documented business justification. Default admin passwords changed on all routers and firewalls.
Secure Configuration	Unused software and services removed or disabled. Default accounts deleted or disabled. Software extensions/plugins reviewed. Least-privilege principle applied to all accounts.
MFA — AUTO-FAIL RISK	MFA enabled on ALL cloud services (Microsoft 365, Google Workspace, CRM, accounting, file storage, etc.). MFA enabled for all admin accounts.

Control area	Confirm before submitting
	BYOD devices accessing data have MFA enforced. Passwordless or FIDO2 options configured where available.
Patching — AUTO-FAIL RISK	All devices have high/critical patches applied within 14 days. Coverage includes OS, third-party apps, browsers, and firmware. Router and firewall firmware is current. Patch dates can be evidenced if required for CE+.
Malware Protection	Active malware protection running on all in-scope devices. Signatures/definitions updating automatically. Software application controls in place where anti-malware is not used.
Scope	All cloud services storing/processing business data are declared in scope. BYOD devices accessing business data included or restricted. Home and remote working devices in scope. No scope exclusions that cannot be justified by technical segregation.
User Access Control	Admin and standard user accounts are separate. Shared accounts removed or justified. Leaver accounts disabled promptly. Service accounts reviewed and restricted.

The Certification Process: Step by Step

Here's what to expect from start to certificate, for both tiers:

Cyber Essentials (Self-Assessment)

- **Step 1:** Download and review the v3.3 Requirements for IT Infrastructure document and the Danzell question set from the IASME website. Complete a dry run in a spreadsheet before purchasing the portal.
- **Step 2:** Purchase your assessment through an IASME-accredited Certification Body. Cost is typically £320–£440 for organisations up to 50 users.
- **Step 3:** Complete the Danzell self-assessment questionnaire in the online portal, covering all five controls. This typically takes 2–4 hours if your environment is well-documented.
- **Step 4:** Your Certification Body reviews and verifies your answers. They may ask clarifying questions. Turnaround is usually 2–5 business days.
- **Step 5:** On passing, you receive your Cyber Essentials certificate, valid for 12 months.

Cyber Essentials Plus (Technical Audit)

CE+ follows the same process but adds an independent technical assessment by an accredited assessor. Under Danzell, this includes:

- **Internal vulnerability scanning of a representative sample of devices**
- **External vulnerability scanning of your internet-facing perimeter**
- **Verification that MFA is active across cloud services and admin accounts**
- **Confirmation that patch status matches your self-assessment claims**
- **A second device sample (new in Danzell) to verify estate-wide remediation, not just the initial sample**

Timing note:
CE+ must be purchased and commenced within three months of your CE self-assessment. The scope for both must be identical, this is now formally verified under Danzell. Do not attempt CE+ without first completing a thorough internal gap review.

Ready to get certified?

Cyber Essentials is achievable for virtually every SME with the right preparation. Most businesses with modern cloud-based infrastructure, Microsoft 365, a managed device estate, and a sensible patching process are closer than they think. The most common barrier isn't technical complexity; it's simply not knowing what's expected before you start.

We help SMEs across London, Midlands and the South East prepare for, achieve, and maintain Cyber Essentials and Cyber Essentials Plus certification. If you'd like a no-obligation gap assessment against the Danzell (v3.3) requirements, get in touch.

Contact us: hello@urbannetwork.co.uk.co.uk | 0800 000 0000 | urbannetwork.co.uk

Official resources: ncsc.gov.uk/cyberessentials | iasme.co.uk/cyber-essentials