CyberSmart

Upcoming Changes to Cyber Essentials:

The New Danzell Question Set

The Danzell question set goes live on **26 April 2026**, and there is quite a lot to pay attention to. IASME and the NCSC have introduced auto-fail conditions, tightened the CE Plus assessment process, significantly expanded scope transparency requirements, and updated the declaration directors sign when completing a verified self-assessment. Some of these changes will directly affect whether clients pass or fail. Others change the commercial conversations MSPs can have around ongoing compliance.

This guide covers every significant change and what it means in practice.

The biggest changes: auto-fail questions

The most operationally significant update in Danzell is the introduction of auto-fail conditions. Previously, failing a question didn't automatically end an assessment. Under Danzell, three areas will end it immediately regardless of performance elsewhere.

MFA for cloud services

Multi-factor authentication is now mandatory for all cloud services where it is available. If MFA exists as an option, whether free, included, or paid, and it hasn't been enabled, the assessment fails automatically.

This was signalled in November 2025 when IASME published the updated Requirements for IT Infrastructure document (v3.3), but it is now confirmed as an auto-fail condition in the Danzell question set.

There is no partial credit for having MFA enabled on some services but not others. Every cloud service that offers it must have it turned on. For MSPs managing multiple client environments, this requires a sweep of all cloud services across each account before submission, paying particular attention to services added after the last certification cycle where MFA may not have been configured by default.

One important distinction: if a cloud service has no MFA option at all, that does not trigger an automatic failure. Organisations declare those services at question A7.15, and questions A7.16 and A7.17 explicitly exclude services listed there from the MFA requirement. The auto-fail applies where MFA is available and not enabled. A legacy or niche SaaS tool with no MFA capability at all sits in a different category and must be declared rather than remediated. The practical priority for MSPs is identifying any service where MFA exists but has not been switched on.

Security update management: A6.4 and A6.5

Two questions related to patching and vulnerability fixes are now auto-fail:

A6.4: Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release?

A6.5: Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release?

The 14-day requirement is not new. The auto-fail consequence is. IASME has been explicit about the reasoning: delays in applying critical updates are a primary cause of compromise, and the previous marking approach wasn't creating sufficient urgency.

High-risk or critical updates are defined as those where the vendor describes the vulnerability as critical or high-risk, or where the CVSSv3 base score is 7 or above. This applies across operating systems, router and firewall firmware, and applications including any associated files and extensions.

For clients with manual update processes, inconsistent patching across distributed estates, or legacy systems on extended support programmes, this is the change most likely to cause failures in the first renewal cycle under Danzell.

The updated director declaration

The declaration signed by a board member or director as part of the verified self-assessment will be updated. It will now include a formal acknowledgement that the organisation is responsible for maintaining compliance with all Cyber Essentials controls throughout the certification period, not just at the point of assessment.

Under the previous version, the sign-off was essentially a confirmation that the self-assessment was accurate on a given day. The updated declaration is a commitment about what the organisation will do for the next twelve months.

What this means for MSPs

Getting board-level investment in ongoing security, when the certificate has been issued and there's no incident to point to, has always been a difficult conversation to start. The standard approach is to explain the risk. That works, but it positions the MSP as bringing a problem to the table.

The updated declaration changes the dynamic. The director has signed a specific commitment. The MSP is helping them honour it.

That reframing has practical consequences. Continuous device monitoring, enforced patching, MFA across cloud services, and regular access control reviews are no longer recommendations. They are the infrastructure for meeting an obligation the director has already agreed to. That's a meaningfully different conversation at QBR, at onboarding, and at renewal.

It also creates a natural reason to involve the director directly. They've put their name to something specific. Understanding what that means, and what is in place to support it, is a board-level conversation rather than one for the IT manager alone.

Scope and certification: more detail, more transparency

Scoping has always been one of the more complex parts of Cyber Essentials, particularly for organisations with subsidiaries, multiple sites, or mixed network structures. Danzell introduces several changes here.

Whole organisation vs partial organisation

The A2.1 scoping question has changed format. Previously a Yes/No question about whether the whole organisation was in scope, it is now a multiple-choice question: Whole organisation or Partial organisation.

If a client selects Partial organisation, the assessment account will route them through the additional scoping questions below. This is a process change as much as a requirement change, but it's worth knowing so assessment accounts are set up correctly from the start.

Out-of-scope areas must be documented

If any part of an organisation's infrastructure is excluded from the assessment, those exclusions must now be described in the assessment, including how excluded networks are segregated from in-scope systems. This information will not be made public, but it must be provided.

Two new questions address this directly: A2.2.1 asks for a description of excluded networks, and A2.2.2 asks how sub-sets were created. Subsets must be created using a firewall or VLAN. Security groups, microsegmentation, and software-based methods are not compliant for defining the scope boundary.

Unlimited scope descriptions

Previously, scope descriptions on certificates were limited to 300 characters.
Under Danzell, that limit is removed. Organisations can provide a detailed scope description, accessible via the digital certificate platform. The certificate itself will indicate whether it covers the whole organisation or a partial scope and direct readers to the platform for the full description.

Legal entity identification

All legal entities included within the scope of the assessment must now be specified, with name, address, and company number for each. This information will be visible on the digital certificate platform.

If a scope includes subsidiary companies, they need to be listed explicitly at A1.6 and A1.6.1. The board member signing the assessment must have authority to represent all listed entities. Any legal entities not listed before certification is complete cannot be added retrospectively.

Individual certificates for entities within a larger scope

Organisations can now request an individual Cyber Essentials certificate for each legal entity certified as part of a wider assessment. Each certificate will clearly indicate it is part of a broader scope. There will be a small additional charge per certificate.

'Point-in-time' clarified

The scheme will now explicitly state that the point in time for a Cyber Essentials assessment is the date the certificate is issued. All systems must be supported and compliant as of that date. This resolves a persistent source of ambiguity, particularly around software that may have gone end-of-life between submission and certificate issuance.

Changes to the requirements document

The Requirements for IT Infrastructure v3.3, published in November 2025, includes several updates worth understanding before preparing client assessments.

Cloud services: a formal definition

A clear definition of cloud services has been added:

> A cloud service is an on-demand, scalable service, hosted on shared infrastructure, and accessible via the internet. For the purposes of Cyber Essentials, a cloud service will be accessed via an account and will store or process data for your organisation.

Cloud services cannot be excluded from scope under any circumstances. Social media accounts (LinkedIn, Facebook, X) used for business purposes fall within this definition, as they did under Willow.

One nuance worth understanding for MSPs managing partial scope assessments: only in-scope devices connecting to cloud services need to be included in the assessment itself. However, user accounts that access cloud services from out-of-scope devices are still required to comply with Cyber Essentials controls, including mandatory MFA. The device may be out of scope. The user account accessing organisational cloud services is not. This matters particularly for BYOD arrangements and organisations with mixed estates where some devices are excluded from the certification boundary.

Scoping simplified

The terms 'untrusted' and 'user-initiated' have been removed as qualifiers for internet connections in the scoping criteria. Organisations must now justify any exclusions and explain how excluded networks are segregated from in-scope systems.

Application development (formerly 'web applications')

The 'web applications' section has been renamed 'application development' and now references the UK Government's Software Security Code of Practice. Publicly available commercial web applications remain in scope by default. Bespoke and custom components are out of scope.

Backups

Guidance on backups has been repositioned earlier in the requirements document. The underlying requirements are unchanged.

Passwordless authentication

The user access control section gives greater prominence to passwordless authentication methods, such as passkeys, as a more secure alternative to traditional passwords. This builds on the direction set in Willow, which introduced passwordless as an acceptable method for firewall and router authentication.

Changes to Cyber Essentials Plus

CE Plus sees some of the most substantive process changes in Danzell, with both the sampling methodology and the relationship between the VSA and the audit tightened significantly.

Closing the selective update loophole

IASME's auditors identified a pattern: when organisations failed an initial CE Plus test for update management, some were applying fixes only to the specific devices included in the sample rather than across the entire scope. They would pass the retest without having addressed the wider vulnerability. The certificate was issued against a partially remediated environment.

From April 2026, that approach will not work. If an organisation fails the initial random sample test for update management, the retest will not simply recheck the original sample. The assessor will also test a new, separate random sample. Compliance must hold across both. A second failure will result in revocation of the verified self-assessment certificate.

For MSPs preparing clients for CE Plus, the implication is clear: remediation during the audit process must be applied across the entire in-scope estate, not only to the devices being tested. Anything else is now a revocation risk.

VSA must be finalised before CE Plus testing begins

Organisations will no longer be permitted to adjust their VSA responses based on what they discover during CE Plus testing. The VSA must be complete and finalised before CE Plus testing commences. The scheme's Terms and Conditions will be updated to make this explicit.

The intent is to ensure the CE Plus audit is testing the actual self-assessment, not a version revised in light of audit findings. For MSPs, this means the VSA preparation process needs to be thorough before the audit is booked, not treated as a working draft to be tidied up during the engagement.

New and changed questions in the Danzell question set

Beyond the structural changes above, the question set includes several new questions. Some reflect new requirements, others give assessors better visibility of how an organisation is set up. The ones most relevant for MSPs managing client assessments:

A1.3:

Number of employees, including volunteers, agency workers, and contractors with access to organisational data. Previously absent from the question set.

A1.5 / A1.5.1:

Registered address and operational addresses if different. The address question has been split to distinguish between legal registered address and the locations where the organisation actually operates.

A1.6 / A1.6.1:

Whether the assessment includes more than one legal entity and, if so, the details of each. New questions reflecting the legal entity transparency requirements described above.

A1.12:

Whether an NCSC-assured Cyber Advisor has been consulted. This is a new question and is not a requirement, but assessors will see the answer. For MSPs who are not themselves Cyber Advisors, it is worth understanding whether clients have sought advice elsewhere.

A1.14:

How the organisation heard about Cyber Essentials. A new question, purely for IASME's own research purposes. No action required.

A1.16:

Whether the organisation has signed up to the NCSC's free Early Warning service. Again, not a requirement, but a new question in the set. The Early Warning service notifies organisations of known vulnerabilities and threats relating to their IP addresses and domains. Worth recommending to clients regardless of its presence in the question set.

A2.1:

Format changed from Yes/No to multiple choice (Whole organisation / Partial organisation) as noted above.

A2.3.1 / A2.3.2:

Whether each site has its own internet connection, and if not, how sites are connected to each other. New questions that give assessors visibility of multi-site network topology. Straightforward to answer but worth confirming with clients who have offices sharing a single upstream connection.

A2.4 / A2.4.2:

Networks in scope, and how home and remote workers connect to organisational data and services. The addition of A2.4.2 specifically asks for the connection method (home router, business-provided router, corporate VPN). Assessors are looking for evidence that home and remote working arrangements have been properly considered within the scope, not just acknowledged.

A2.4 / A2.4.2:

For partial organisation assessments, a list of the equipment used to create subsets. New question directly linked to the stricter subset documentation requirements.

When does Danzell take effect?

The Danzell question set applies to all assessment accounts created after 26 April 2026

Organisations with an active assessment account created before that date have six months to complete certification under the previous version of the requirements. For MSPs managing a volume of client assessments, it is worth auditing which accounts are open and at what stage before 26 April, and scheduling renewals accordingly.

What to do now

Sweep MFA across all client cloud services. The auto-fail condition means a single cloud service without MFA enabled will end an assessment. Do this before submission, not during it.

Audit patching processes across your client estate. The 14-day requirement for high-risk and critical updates is now an automatic failure if not met. For clients on manual processes or with large device fleets, this needs to be verified rather than assumed. Also check Windows 10 devices for ESU enrolment: any client running Windows 10 beyond 14 October 2025 without an active Microsoft Extended Security Update subscription is running an unsupported OS, which fails at A6.1 and now also triggers the auto-fail at A6.4.

Prepare CE Plus clients differently. The VSA needs to be complete before the audit is booked. Remediation during the audit must be applied estate-wide, not device-by-device. Walk clients through this before the engagement starts, not after the first sample failure.

Use the director declaration conversation. The updated sign-off is a board-level conversation starter. Directors need to understand what they are committing to, and the MSP is well placed to explain what maintaining compliance throughout the year actually requires. That's an ongoing services conversation, not a compliance admin one.

Review partial scope clients carefully. The new scoping questions require more detail than before. If any client has historically certified as a partial organisation with a minimal scope description, the A2.2.1 and A2.2.2 questions will require more thorough documentation this cycle.

If you'd like to talk through what any of these changes mean for your practice, **get in touch.**

The Danzell question set was published on 13 February 2026 and applies to assessment accounts created after 26 April 2026. The updated Requirements for IT Infrastructure v3.3 are available on the NCSC website.