Cyber Essentials v3.3
What changed?

Cubit TECHNOLOGY

Cyber Essentials has now moved to version 3.3. The new question set is called Danzell. The five core controls have not changed, but the way they are assessed is stricter. Several things that were previously flagged as non-conformities are now automatic failures.

Four changes you need to know:

MFA is now mandatory

If a cloud service offers multi-factor authentication and it is not enabled for all users, the assessment is an automatic failure. No exceptions. This covers Microsoft 365, Google Workspace, Slack, Dropbox, Adobe, and any other cloud platform accessed through an organisational account, including social media.

14-day patching is an auto-fail

Any high or critical vulnerability older than 14 days fails the assessment outright. This applies to operating systems, applications, and firewall firmware. There is no remediation window once the audit has started.

CE Plus now uses double sampling

If the assessor finds a patching failure, they take a second independent sample across the full estate. A second failure revokes the certificate entirely.

Directors are personally accountable

A board member or director must sign a declaration committing the organisation to maintaining CE controls for the full 12-month certification period. IASME can investigate post-certification and revoke the badge if controls have lapsed.

Already have Cyber Essentials?

Your current certificate remains valid. When you renew, your assessment will use the Danzell criteria. We recommend starting preparation at least eight to ten weeks before your renewal date.

Cubit TECHNOLOGY

We review your setup against Danzell before you open an assessment account, fix the gaps, and keep your systems at the certified standard between renewals. **Speak with a member of our team today.**