Idela
Securing Tomorrow, Today.

The 7 Deadly Sins of Cyber Essentials Certification

Why SMEs Fail Certification — And How to Avoid It

Cyber Essentials isn't complicated, but SMEs make the same mistakes repeatedly. This guide identifies the seven critical failure points we see most often—and shows you how to avoid them.

SIN #1: Misunderstanding Scope

The Mistake:

Organisations think CE certification means 'our main office computers.' They exclude home-working laptops, mobile devices, cloud systems, and remote infrastructure.

Why It Matters:

CE scope is ALL devices connecting to the internet for business use. Get this wrong and your submission gets sent back for complete rescoping.

Quick Fix:

Map your complete digital estate before starting. Include office devices, remote workers, mobile phones, tablets, servers, and cloud services. When in doubt, include it.

SIN #2: The MSP Illusion

The Mistake:

"Our IT provider handles everything, so we're fine." Organisations assume their MSP has certification covered without verifying documentation exists.

Why It Matters:

CE certifies YOUR organisation, not your MSP. You must provide evidence of controls. If your MSP can't or won't provide certification-ready documentation, your submission stalls.

Quick Fix:

Engage your MSP early. Confirm they can provide firewall configs, patch management docs, and access control policies in certification-ready format.

SIN #3: Patch Management Theatre

The Mistake:

"Updates are automatic, so we're compliant." Organisations rely on Windows Update without visibility, documentation, or evidence.

Why It Matters:

CE requires proof that security patches are applied within 14 days, across your entire estate, with documented exception handling. Automatic updates alone aren't sufficient.

Quick Fix:

Implement patch visibility tools. Document your review and deployment process. Track compliance across your estate. Ensure you can produce evidence of timely patching.

SIN #4: MFA Misconfiguration

The Mistake:

Organisations enable MFA but don't configure it correctly—partial coverage, weak methods (SMS), undocumented exceptions, or conditional access that barely triggers.

Why It Matters:

CE requires MFA for all remote access and all admin accounts, using robust methods. Gaps in coverage or weak implementation fail the control.

Quick Fix:

Audit MFA comprehensively. Cover all remote access points and admin accounts. Use app-based or hardware tokens where possible. Document any exceptions with business justification.

SIN #5: Shared Account Chaos

The Mistake:

Shared accounts exist 'for good reasons'—info@ email, generic admin login, communal office tablet. Organisations don't see these as compliance failures.

Why It Matters:

CE explicitly prohibits shared accounts. Every user must have a unique account for accountability. Even one shared account means you fail user access control.

Quick Fix:

Audit for shared credentials and eliminate them. Use shared mailboxes accessed via individual accounts, not shared logins. Implement proper user access reviews.

SIN #6: The Router Isn't a Firewall

The Mistake:

"We have a router from our ISP with built-in firewall, so we're compliant." Organisations confuse consumer routers with properly configured boundary firewalls.

Why It Matters:

CE requires deny-by-default firewall configuration with documented rulesets and regular reviews. Default router configs often allow unnecessary services (UPnP, remote management).

Quick Fix:

Review boundary firewall actively. Lock down unnecessary services. Document your ruleset and business justification for allowed services. Implement network segmentation (e.g., guest WiFi isolated).

SIN #7: Time Pressure Syndrome

The Mistake:

"We need certification by next week for a tender." Organisations rush submission without preparation and expect immediate certification.

Why It Matters:

CE is a technical assessment requiring proper preparation—scoping, gap identification, evidence gathering. Rushed submissions lead to lengthy back-and-forth or missed deadlines.

Quick Fix:

Plan ahead. Give yourself 4-6 weeks runway. Conduct a readiness assessment first to identify gaps before formal submission.

Ready to Get Certified?

At Idela, we help SMEs achieve Cyber Essentials certification first time—without the confusion and back-and-forth pain of failed submissions.

Our readiness-first approach identifies gaps before formal assessment, so you submit when you're genuinely ready.

READINESS VALIDATION	STRUCTURED ASSESSMENT	COMPREHENSIVE PATHWAY
For organisations mostly ready	For organisations needing guidance	For organisations starting from low maturity
Quick validation call	Gap assessment + documentation support	End-to-end handholding
From £950	From £1,750	From £3,500

Start with a Free 15-Minute Readiness Call

No obligation. No sales pressure. Just clear guidance on where you stand.

letstalk@idelaonline.com | +44 20 7946 0958
www.idelaonline.com

Idela is an IASME-approved Certification Body specialising in Cyber Essentials and IASME Cyber Assurance for UK organisations.