

Cyber Essentials FastTrack

Rapid Cyber Essentials readiness and certification support

Introduction

Cyber Essentials has moved from a nice-to-have to a hard requirement across a growing number of sectors. Public sector contracts increasingly mandate it as a condition of procurement. Cyber insurers are using it as a baseline for underwriting decisions. Enterprise customers are asking suppliers to hold it as part of supply chain assurance programmes.

Yet for many organisations, the path to certification is unclear. Internal teams know what they need to do in principle but lack the structured time, the specific technical knowledge, or the independent view to get there without delays and failed attempts.

The cost of those delays is rising. A lost public sector bid, a refused insurance application, or a failed supplier audit can each carry financial implications that far exceed the cost of getting certified properly in the first place.

The Challenge

58% of UK SME's that attempted Cyber Essentials certification in the past 3 years required remediation work before they could pass, with common failure points including patch management gaps, misconfigured firewalls and uncontrolled user access privileges.

Additionally, over 40% of organisations that hold a Cyber Essentials certification failed to maintain it at renewal, typically because the controls that passed the initial assessment drifted over time without ongoing governance.

The UK government now mandates Cyber Essentials for all suppliers handling personal data or providing technical products and services under government contracts, a requirement that now flows down through supply chains to thousands of businesses that may not yet realise they are affected.

These statistics point to a single underlying truth: most organisations don't fail to certify because their security is fundamentally poor. They fail because they approach certification without a structured readiness process.

The gap between where they are and where they need to be is usually smaller than it appears, but without expert guidance, it can take far longer to close than it should.

What our customers say about this service

"We'd been putting off Cyber Essentials for over a year because it felt like a bigger project than our team could take on. Cyberfort had us ready in a matter of weeks. The gap analysis was eye-opening. Most of the issues were straightforward to fix once someone had actually mapped them out."

IT Manager, Professional Services Firm

"Our largest customer made Cyber Essentials a contractual requirement with 60 days' notice. Cyberfort got us through it with time to spare. The policy templates alone saved us days of work."

Operations Director, Technology Reseller

"We'd failed a previous attempt through a different provider. Cyberfort identified exactly why and we passed at the first attempt this time. The process was well-structured and the team kept it moving."

Head of IT, Regional Healthcare Business

Typical scenarios where an organisation may need this service include



A public sector tender requires Cyber Essentials as a condition of bidding.



A customer or partner has asked for evidence of certification.



Your cyber insurer has flagged it as a requirement at renewal.



Your organisation has grown and your IT environment has changed significantly since you last assessed your baseline controls.



You are preparing for a due diligence review as part of an M&A process.



You have tried to certify before and been declined or deferred.



Your IT team has changed and there is no clear owner for the certification process.

Who is this service for?



This service is designed for **IT Directors, Operations Directors, Compliance Managers and business owners** responsible for meeting customer, procurement or regulatory requirements.

Ask yourself: Has a customer, insurer or public sector body asked you for Cyber Essentials certification? Are you unsure whether you would pass an assessment today? Is your team stretched and unlikely to get there without structured support?

If any of these apply, this service is for you.

What does a typical engagement for this service look like?

1

Step 1 - Scoping & Kickoff

We agree the scope of the assessment, which systems, networks and locations are in scope and brief your internal team on what to expect. We establish a clear picture of your current environment and identify the five control areas we will assess: firewalls, secure configuration, user access control, malware protection and patch management.

2

Step 2 - Gap Analysis

We conduct a structured review of your current controls against the Cyber Essentials standard. We identify every gap, score it by severity and produce a prioritised remediation list that separates what needs fixing before certification from what can be addressed as good practice afterwards.

3

Step 3 - Guided Remediation

We work alongside your team to close the priority gaps. Where policy documentation is needed, we provide ready-to-use templates. Where technical configuration changes are required, we provide clear guidance and validate the outcome. We keep the process practical and focused, no unnecessary work, no scope creep.

4

Step 4 - Certification Support & Executive Summary

We support you through the formal assessment process, liaising with the certifying body where needed and providing a clear Executive Compliance Summary for board or senior stakeholder reporting. Where a Cyber Essentials Plus assessment is the target, we scope and prepare for the additional verification requirements at this stage.

Key Deliverables

-  Gap Analysis Report
-  Prioritised Remediation Plan
-  Policy Templates (firewall, access control, patching, malware)
-  Certification Support
-  Executive Compliance Summary

Business Value

-  Achieve certification readiness without failed attempts or wasted effort
-  Satisfy public sector, customer and insurer requirements quickly
-  Improve your baseline cyber hygiene across the five core control areas
-  Give your board and your customers a credible, independently verified security baseline
-  Reduce the risk of losing contracts or insurance cover due to a missing certification

Key outcomes from this service

By the end of the engagement, you will have a clear understanding of your current baseline security posture, a fully remediated environment ready for Cyber Essentials assessment, policy documentation that satisfies both the certification requirements and your internal governance needs, and an Executive Compliance Summary suitable for board reporting, customer assurance or insurer submission.

Why choose Cyberfort for Cyber Essentials

Cyberfort's consultants have guided organisations through Cyber Essentials and Cyber Essentials Plus assessments across financial services, professional services, manufacturing, and public sector supply chains since its inception as a standard.

We understand the practical gaps that cause assessments to fail and the fastest routes to closing them. We are also accredited to support onward assessments for Cyber Essentials Plus, meaning the work done here can directly underpin a more comprehensive assurance programme if needed.



Book Your Cyber Essentials Readiness Call

Don't let a missing certification cost you a contract, an insurance renewal or a supplier relationship. Book a 30-minute call with one of our Cyber Essentials specialists to understand exactly where you stand today, what needs to change, and how quickly we can get you to certification-ready.

To book your appointment simply email us at info@cyberfortgroup.com.

To find out more about our security services visit cyberfortgroup.com.