Cyber Essentials

Cyber Essentials — Client Guide
IASME-licensed Certification Body

The Rybec Group
contact@rybec.co.uk
www.rybec.co.uk

What is Cyber Essentials?

Cyber Essentials is the UK Government-backed certification scheme that sets the minimum baseline standard for cyber security. It was developed with the National Cyber Security Centre (NCSC) and is built around five technical controls that protect organisation's against the most common internet-based cyber-attacks.

Those five controls are: firewalls, secure configuration, user access control, malware protection, and security update management.

Most cyber-attacks on UK businesses are not sophisticated. They are opportunistic — the digital equivalent of a burglar walking down a street trying door handles. The five Cyber Essentials controls are designed to make sure your doors are locked. Implemented properly, they stop the large majority of everyday attacks before they start.

That's the point worth holding onto: Cyber Essentials is a practical security improvement framework. The certificate is evidence that the work has been done — not a substitute for doing it.

Why do organisations get certified?

Because a customer or contract requires it. Cyber Essentials is required in a large number of central government contracts and is mandatory for Ministry of Defence suppliers handling defence information. Increasingly, larger businesses ask for it from their suppliers too.

Because it genuinely reduces risk. The controls address the attack methods that actually hit UK organisations — phishing-delivered malware, exploitation of unpatched software, and compromised accounts.

Because it demonstrates credibility. Certification shows clients, partners and insurers that your organisation takes security seriously, backed by an independent assessment rather than your own say-so. Eligible UK organisations that certify also receive included cyber liability insurance as part of the scheme.

How the process works

1. Prepare. Download the current question set and the Requirements for IT Infrastructure document from the IASME website and review your organisation against them. This is where most of the real

work happens, understanding what devices, software, cloud services and user accounts are in scope, and whether your controls meet the standard.

2. Complete the self-assessment. You answer a structured questionnaire about your organisation's IT — covering devices, cloud services, access controls, malware protection and how you apply security updates. A board member or senior equivalent must confirm the answers are accurate before submission and acknowledge the organisation's responsibility to maintain the controls throughout the certification period — not just on assessment day.

3. Assessment. A qualified assessor from a licensed Certification Body reviews your answers. If clarification is needed, you can update and resubmit.

4. Certification. Once your assessment meets all requirements, your certificate is issued and you receive a digital badge to display. The certificate is valid for 12 months, and annual renewal keeps your certification — and your controls — current.

What changed in April 2026

The Cyber Essentials requirements are reviewed and updated annually by the NCSC and IASME. The latest version — Requirements for IT Infrastructure v3.3 — applies to all assessment accounts created after 27 April 2026. The changes worth knowing about:

Cloud services cannot be excluded from scope. If your organisation's data or services are hosted in the cloud — Microsoft 365, Google Workspace, accounting platforms, CRM systems — those services are in scope. For most modern SMEs, the cloud is the IT estate, so this matters.

Multi-factor authentication is now a hard line. If a cloud service you use offers MFA and it is not enabled for all users, the assessment fails automatically — regardless of how strong everything else is. The scheme also formally recognises passwordless sign-in methods such as passkeys, which the NCSC would like to see become the default way people log in. If MFA is not yet switched on across every cloud service your business uses, that is the first thing to fix.

Security updates are the other hard line. High-risk and critical security updates must be applied within 14 days of release — across operating systems, router and firewall firmware, and applications. Failing this also fails the assessment automatically. Fourteen days is not a target; it is the line.

If your renewal is coming up, it's worth reviewing your MFA coverage and patching process well before you start the assessment. These two auto-fail rules are where organisations are most likely to be caught out.

Common misconceptions

“We're too small to be a target.” Attackers don't choose targets the way you might imagine. Automated attacks scan for weaknesses, not company size. Small organisations are often hit precisely because attackers expect weaker defences.

“We passed last year, so we'll pass this year.” The requirements evolve annually, and your IT estate changes too — new starters, new devices, new cloud services. Each renewal is a genuine reassessment.

“It's just paperwork.” Answered honestly, the questionnaire tests whether real controls are in place on real systems. Organisations that treat it as a form-filling exercise tend to discover their gaps at the worst possible moment.

How The Rybec Group can help

The Rybec Group is an IASME-licensed Certification Body. We assess and issue Cyber Essentials certificates directly — no third parties, no hand-offs.

We also offer consultancy support as a distinct service for organisations that want guidance through the process: helping you understand what each question is really asking, checking your setup against the requirements, and completing the self-assessment questionnaire with you. If gaps are identified along the way, we can provide remediation guidance as a separately scoped piece of work — so you always know exactly what's being done and why.

Our founders spent decades investigating crime in UK policing. We've seen how attacks actually happen, and we built Rybec to help businesses close the gaps that let them happen.

Questions? Get in touch: contact@rybec.co.uk | www.rybec.co.uk