Cyber Essentials Plus

Cyber Essentials Plus — Client Guide
IASME-licensed Certification Body

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

What is Cyber Essentials Plus?

Cyber Essentials Plus is the audited tier of the Cyber Essentials scheme. The technical controls are exactly the same as standard Cyber Essentials — firewalls, secure configuration, user access control, malware protection, and security update management. The difference is the level of assurance.

Standard Cyber Essentials is a verified self-assessment: you declare that the controls are in place, and an assessor reviews your answers. Cyber Essentials Plus adds an independent technical audit of your actual systems to verify the controls are working in practice.

Put simply: Cyber Essentials says the controls exist. Cyber Essentials Plus proves it.

Why do organisations choose Plus?

Supply chain and procurement requirements. Government contracts, defence supply chains and larger enterprise customers increasingly specify Cyber Essentials Plus rather than the standard certification, because independently verified evidence carries more weight than self-declaration.

Genuine confidence in your own controls. Many organisation's believe their controls are in place until someone tests them. The Plus audit finds the gap between what your policies say and what your systems actually do, which is exactly the gap attackers look for.

A stronger signal to clients and insurers. A certificate backed by independent technical testing tells a more convincing story than one based on self-assessment alone.

How the process works

1. Achieve Cyber Essentials first. A valid Cyber Essentials certificate is the prerequisite. The Plus audit verifies the same controls, so the self-assessment stage has to be complete and passed first.

2. Book the audit within the three-month window. The Plus audit must be completed within three months of your Cyber Essentials certification. This matters for planning: if you certify Cyber Essentials in the spring and leave the Plus audit until the autumn, you will need to pass the self-assessment again first. The cleanest approach is to plan both stages as one project.

3. The technical audit. An assessor from a licensed Certification Body carries out a technical audit of your systems. This covers a representative sample of user devices, all internet gateways, and all servers with services accessible from the internet. It includes vulnerability scanning and checks that protections such as malware defences behave the way they should. Audits can be carried out remotely or in person, depending on your environment.

4. Findings and verification. The assessor confirms whether the controls tested match the standard. Where issues are found, you'll understand exactly what they are and why they matter.

5. Certification. Pass the audit and your Cyber Essentials Plus certificate is issued, valid for 12 months alongside the annual renewal cycle.

What the audit typically reveals

In our experience as a Certification Body, the organisations that find Plus most valuable aren't the ones with terrible security — they're the ones who assumed everything was fine. Common findings include devices missing critical updates that “should” have been applied automatically, malware protection installed but misconfigured, and user accounts with more privilege than anyone realised.

None of these show up on paper. All of them show up under testing. That's the value of Plus: it replaces assumption with evidence.

Preparing for a first Plus audit

The best preparation is honest housekeeping before the audit rather than during it. Know what devices you have and confirm they're all supported and up to date. Check that security updates are actually being applied within the required 14-day window, not just scheduled. Confirm MFA is enabled across your cloud services. Make sure malware protection is present and correctly configured on every in-scope device.

Organisations that do this groundwork tend to pass the first time. Organisations that treat the audit as the discovery exercise tend not to.

How The Rybec Group can help

The Rybec Group is an IASME-licensed Certification Body for both Cyber Essentials and Cyber Essentials Plus. We deliver the full journey in-house — one accountable partner from preparation through to certificate. That includes sequencing the self-assessment and the Plus audit, so the three-month window never becomes a problem.

For organisations that want support before the audit, our consultancy service covers readiness: reviewing your devices, configurations and cloud services against what the audit will actually test, so there are no surprises on the day. Where preparation or the audit itself identifies issues, remediation guidance is available as a separately scoped piece of work.

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