



COMPLIANCE RESOURCE

Cyber Essentials Prep Checklist

A floor, not a ceiling. Cyber Essentials verifies five technical controls against the most common internet-based attacks. This checklist helps you reach it in weeks, not months.

For IT teams in Ireland and the UK
Prepared by the Edge7 Networks Compliance Practice

Before you start

Cyber Essentials is a UK government-backed scheme, run by IASME on behalf of the National Cyber Security Centre. Rather than assessing your whole management system, it checks that five technical controls are in place to defend against the most common internet-based attacks. It is a strong baseline most organisations can reach in weeks.

Know the current bar

Requirements sit under version 3.3, assessed through the “Danzell” question set introduced in April 2026. Among other changes it treats multi-factor authentication as an auto-fail where it is available but not enabled. The bar rises on a regular cycle as common attacks evolve, so prepare against the current requirements.

The five controls

Work through each control and confirm it is in place across the scope you intend to certify.

- ☐ **Firewalls**
Boundary firewalls between your network and the internet, correctly configured, with default credentials changed.
- ☐ **Secure configuration**
Devices and software hardened: unnecessary accounts and services removed, default passwords changed.
- ☐ **Security update management**
Systems kept patched and supported; unsupported software removed. Critical updates applied promptly.
- ☐ **User access control**
Access and administrative rights limited to what each person needs, with admin accounts used only for admin tasks.
- ☐ **Malware protection**
Malware protection in place and current across in-scope devices.

MFA is now a hard requirement

Under the current question set, MFA available but not enabled is an auto-fail. Enable multi-factor authentication everywhere it is offered, especially for cloud services and administrative access, before you submit.

Base certification or Plus?

Two levels

Cyber Essentials a verified self-assessment against the five controls. Reachable in weeks and strong for UK public sector and supply-chain requirements.

Cyber Essentials Plus adds an independent technical audit, where an assessor tests the controls rather than taking your word for them. Plan for the audit once the base controls are solid.

Cyber Essentials is designed to stop the bulk of commodity attacks, the automated, opportunistic threats that make up most of what any organisation faces. It is a floor, not a complete information security programme, and it is not trying to be. If you need a full management system, ISO 27001 is the next step up.

- ☐ Certification scope defined (which devices, users, and locations are included)
- ☐ All five controls confirmed in place across that scope
- ☐ MFA enabled everywhere it is available
- ☐ Self-assessment completed, or Plus audit scheduled

Preparing for Cyber Essentials? Let's talk.

Edge7 Networks helps IT teams across Ireland and the UK reach Cyber Essentials and Cyber Essentials Plus, and step up to ISO 27001 where it is needed.

Web edge7networks.com **Dublin** +353 1 969 4001 **London** +44 20 8176 0150

This checklist is a practical planning aid produced by Edge7 Networks. Scheme requirements are stated at the time of writing and change on a regular cycle; confirm the current requirements with your certification body. Edge7 Networks holds ISO 27001:2022, ISO 9001:2015, and Cyber Essentials certifications.