What Cyber Essentials *proves*, and what it doesn't.

Cyber Essentials is the UK government-backed baseline against the most common internet attacks. It is increasingly a condition of contracts, tenders and insurance. Directors should know what the certificate tells them, and what it leaves out.

WHAT IT PROVES

Five controls were in place. Firewalls, secure configuration, user access control, malware protection and security update management, across the devices and cloud services in scope.

Against a published standard. Your answers were assessed by an independent certification body, not marked by your own team.

A requirement met. Many customers, public sector contracts and insurers now ask for it before they will work with you.

WHAT IT DOESN'T

That the controls stayed in place. The certificate reflects the day of assessment, and is renewed each year.

That everything was covered. Read the scope. A certificate can leave parts of the organisation out.

Detection, response or recovery. Backups, incident plans, suppliers and governance sit outside it. That is where ISO 27001 and a tested response plan come in.

Hands-on testing. The standard certificate is assessed from your answers. Independent technical testing is Cyber Essentials Plus.

THE FIVE CONTROLS

01 Firewalls

Only the connections you need, in and out.

02 Secure configuration

Defaults removed, nothing running that is not needed.

03 User access control

The right access for each person, and admin rights kept to a few.

04 Malware protection

Every device protected against malicious software.

05 Security updates

High-risk fixes applied within fourteen days.

Five questions *for the board.*

1 **What exactly is in scope, and what was left out?**

A narrow scope is the most common way a certificate says less than it seems.

2 **Who owns each of the five controls between assessments?**

Controls drift. Each one needs a named owner, not just a pass on the day.

3 **When does our certificate expire, and who is preparing the renewal?**

A lapsed certificate can quietly put a contract or an insurance policy at risk.

4 **Do our critical suppliers hold Cyber Essentials, and have we asked?**

Many breaches start with a supplier. It is a reasonable minimum to expect.

5 **Is Cyber Essentials our ceiling, or our first step towards ISO 27001?**

The answer depends on who you sell to and what you hold. It should be a decision, not a default.

FIRST STEP FUND

Eligible UK organisations with fewer than 250 staff that have not held Cyber Essentials in the last four years can get 75% off the certification fee. Buy by 31 March 2027, or sooner if the funding runs out.

75%
Off the fee

Privion.

privion.co.uk/services/cyber-essentials
enquiries@privion.co.uk · 020 3095 6789