



cyberlab

Getting the Basics Right: Your Guide to Cyber Essentials & Cyber Essentials Plus

The UK Government-Backed Standard Explained



Tales from the CyberLab | Episode 22

Cyber Essentials: Common Cyber Threats Explained with IASME

Featuring Neil Furminger, Head of Cyber Essentials at IASME

Why are the same cyber threats from a decade ago still affecting UK organisations today? Our Sales Director Adam Myers sits down with Neil to explore why basic security controls remain the most powerful defence available.

In this episode we cover:

- The origin story of Cyber Essentials and why it was created
- The five technical controls that help prevent around 80% of common cyber attacks
- When to step up from Cyber Essentials to Cyber Essentials Plus

Watch or listen at cyberlab.co.uk or scan the QR code



Introduction

Most cyber attacks are not sophisticated. They rely on freely available tools that scan the internet for unpatched software, weak passwords and poorly configured devices. They are untargeted, they are automated, and they are preventable.

Cyber Essentials is the UK Government-backed certification scheme designed to stop exactly these attacks. Built on guidance from the National Cyber Security Centre (NCSC), it gives organisations of every size a clear, achievable baseline for cyber security, and a recognised way to prove it to customers, partners and public sector buyers.

This whitepaper explains what Cyber Essentials is and where it came from. It covers the five technical controls at its core and how Cyber Essentials Plus adds independent technical assurance. It also explains how to choose the right level for your organisation.

Contents

04	What Is Cyber Essentials?
06	The Five Technical Controls
08	Why Cyber Essentials?
09	Why Cyber Essentials Plus?
10	Cyber Essentials vs Cyber Essentials Plus
11	Preparing for Certification
12	Why Certify with CyberLab?
14	In Conclusion

What Is Cyber Essentials?

A Scheme Built to Stop Everyday Attacks

Cyber Essentials is a UK Government-backed certification that helps organisations protect themselves against the most common cyber threats. It is delivered by IASME, the NCSC's official delivery partner for the scheme, through a UK-wide network of approved Certification Bodies.



Where it began

Around 2010 and 2011, a number of large contractors working for defence and UK Government were being compromised. These were not advanced, targeted attacks. They used commodity tools that anyone could obtain.

In response, CESG, the forerunner of the NCSC, worked with government departments to build a scheme that could prevent them. The team started from the controls in the 10 Steps to Cyber Security.

From these, they selected the five that most effectively stopped these attacks and built Cyber Essentials around them. The scheme launched in 2014.

Since then, it has been a requirement for central government contracts that handle personal data. The controls have adapted to cloud services, remote working and new technology, but the fundamentals have stayed the same.

“ *Many cyber attacks start with freely available tools... We're not looking at the targeted attacks. Cyber Essentials is the untargeted attacks.*

Neil Furminger, Head of Cyber Essentials, IASME



The Threat Model

Cyber Essentials focuses on the attacks organisations face every day. Applied correctly, its controls also help prevent the most common forms of ransomware.

80%

of common cyber attacks
prevented by the five
controls

2014

the year the scheme
launched

2

levels of certification

12

months before renewal

The five controls have been part of IT systems for decades. Getting them right consistently is what makes the difference.

The attacks Cyber Essentials is built to stop

Phishing: emails that trick users into revealing credentials or running malicious files.

Vulnerability exploitation: attackers taking advantage of unpatched software and devices.

Password guessing: automated attempts to access accounts protected by weak or default passwords.

Source: UK Government, Cyber Essentials scheme

The Five Technical Controls

Simple Controls, Significant Protection

Cyber Essentials is built on five technical controls. Each can be applied to a single laptop or across thousands of devices, which is why the scheme works for organisations of any size.



1. Firewalls

A firewall creates a boundary between your devices and the internet, whether on the device itself, at your network edge or in your cloud services.

The requirement: firewalls are configured and in use on every in-scope device, particularly those connecting to public or untrusted Wi-Fi.



2. Secure Configuration

Default settings are designed for convenience, not security. Removing software you don't use, disabling unused accounts and changing default passwords closes unnecessary doors.

The requirement: only necessary software, accounts and services are enabled.



3. Security Update Management

Unpatched software is one of the most common ways in.

The requirement: devices, software and apps are kept up to date and supported. Critical and high-risk updates are applied within 14 days of release, and unsupported software is removed.

Maintain it all year

Cyber Essentials should be maintained 365 days a year. Treating it as a once-a-year exercise for a contract leaves organisations exposed for the other 364.



*Apply all five controls.
Follow the guidance of
the NCSC... it's as simple
as that.*

Neil Furminger, IASME



4. User Access Control

Everyday tasks like email and documents should run from a standard account. Administrator rights belong in a separate account, used only when needed.

The requirement: access is controlled through individual user accounts, with admin privileges given only to those who need them.



5. Malware Protection

Modern malware protection scans devices, checks suspicious links and blocks threats before they run.

The requirement: malware protection is in place, configured to vendor best practice and kept up to date.

Why Cyber Essentials?

A Recognised Foundation for Your Security

Cyber Essentials is the first rung on the ladder to stronger cyber security. It gives you a clear benchmark, and gives your customers a clear signal.



Formalise your security

Gain a clear picture of your cyber security posture, with key processes and policies documented.



Win more business

Cyber Essentials is required for many public sector contracts, and a growing number of private sector buyers now expect it from suppliers.



Set yourself apart

Show customers and partners that cyber security is a priority for your organisation.



Strengthen your supply chain

Weak links anywhere in a supply chain create risk for everyone. Certification demonstrates you are a trusted partner.



Cyber liability insurance

Eligible organisations with a turnover below £20m receive cyber liability insurance, including a 24-hour helpline and incident response support up to £25,000.



Peace of mind

Focus on your organisation's goals, knowing the most common attacks are covered.

What changed in 2026?

From 27 April 2026, new assessments use the Danzell question set, based on Requirements for IT Infrastructure v3.3. It sets tighter expectations around cloud security, authentication and patching.

[Read our Danzell guide](#)



Why Cyber Essentials Plus?

Independent Proof That Your Controls Work

Cyber Essentials confirms you have the right controls in place. Cyber Essentials Plus proves it. A qualified assessor tests your systems directly, giving customers and regulators the highest level of assurance the scheme offers.



When to consider Cyber Essentials Plus

- You are bidding for Ministry of Defence (MoD) contracts or public sector frameworks that specify it
- Your customers or supply chain partners require a higher level of assurance
- You operate in a regulated or higher-risk sector
- You want independent confirmation that your controls work as intended

The Cyber Essentials Plus process

- 01 Remote audit:** A CyberLab assessor reviews the configuration of a sample of devices across your organisation.
- 02 Vulnerability assessment:** We confirm patching and configuration meet the required standard.
- 03 External port scan:** We scan your internet-facing IP addresses for obvious vulnerabilities and misconfigurations.
- 04 Email and web testing:** We test how well your email clients and browsers stop potentially malicious files from running.
- 05 Documentation:** We record evidence of compliance throughout.
- 06 Renewal:** We contact you ahead of your anniversary to keep you certified year after year.

Cyber Essentials Plus must be achieved within 90 days of Cyber Essentials certification.

Book Your Cyber Essentials Plus Audit

Find out what's involved for your organisation.



Cyber Essentials vs Cyber Essentials Plus

Which Level Is Right for You?

	 Cyber Essentials	 Cyber Essentials Plus
Assessment type	Verified self-assessment	Self-assessment plus hands-on technical audit
Verified by	IASME-approved assessor reviews your answers	Assessor reviews your answers and tests your systems
Prerequisite	None	Valid Cyber Essentials certificate. Cyber Essentials Plus must be achieved within 90 days of Cyber Essentials certification.
Vulnerability assessment	✗	✓
External port scan	✗	✓
Email and browser testing	✗	✓
Cloud service checks	Declared in questionnaire	Tested
Level of assurance	Strong baseline	Highest under the scheme
Commonly required for	Central government contracts handling personal data	MoD contracts, public sector frameworks, supply chain requirements
Cyber liability insurance	Included for eligible organisations	Included for eligible organisations
Turnaround with CyberLab	Typically reviewed within 2 working days of submission	Scheduled once Cyber Essentials is in place
Renewal	Annual	Annual
From	£320 + VAT	£1,395 + VAT

Cyber Essentials pricing is set by IASME and varies by organisation size. Pricing aligns with NCSC recommendations.

Preparing for Certification

Five Steps to Pass First Time

1

Define your scope: Identify the devices, networks and cloud services in scope, including those used for home working.

2

Review the question set: Download the current Danzell question set and work through it before you submit.

3

Check your patching: Confirm critical and high-risk updates are applied within 14 days, and remove or replace unsupported software.

4

Separate admin accounts: Make sure no one uses an administrator account for everyday tasks.

5

Get a pre-assessment check: Our assessors can review your answers before submission, so you can fix gaps rather than fail.



Download the Cyber Essentials Question Set

Know exactly what you'll be asked.



Why Certify with CyberLab?

Your Trusted Partner for Cyber Essentials

As an IASME-approved Certification Body for both Cyber Essentials and Cyber Essentials Plus, we don't just assess you against the scheme. We guide you through it, from first questions to renewal.

1,500+

Cyber Essentials and
Cyber Essentials Plus
certifications delivered

4.9/5

Trustpilot rating from
220+ reviews

2

working days to review
your Cyber Essentials
submission

100%

UK-based, IASME-
qualified experts



4.9



223+ reviews

★ Trustpilot



Certify and support

We are authorised to certify your organisation and to help you get there, with pre-assessment checks and remote consultancy.



Pass first time

Our assessors identify gaps before submission, so certification is a smooth process rather than a test.



Transparent pricing

Certification on its own, with a pre-assessment check, or with additional expert support. You choose the level you need.

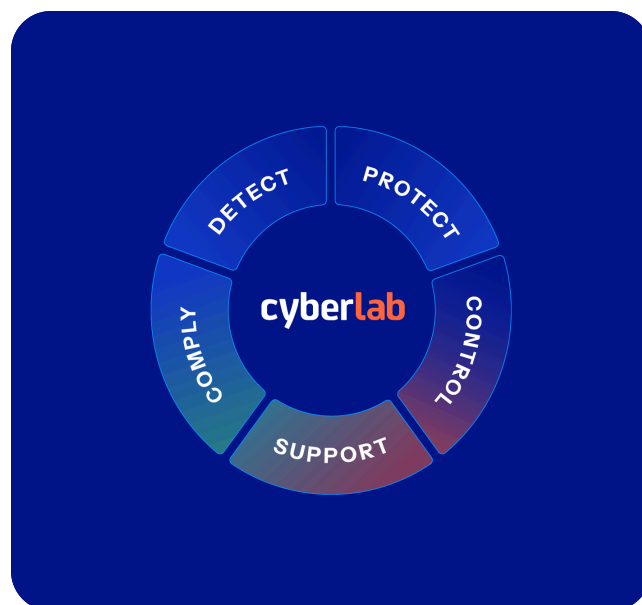


We remember so you don't

We contact you ahead of renewal and guide you through each annual recertification.

Beyond certification

Cyber Essentials is a strong starting point, not the finish line. As a CREST- and CHECK-accredited consultancy and NCSC Cyber Advisor, we help you build on your certification with penetration testing, managed detection and response, and ongoing security support.



Working with CyberLab gave us reassurance that our business meets the highest security standards. Their professional, consultative approach made the Cyber Essentials journey straightforward and added real value to our organisation.

GM61



In Conclusion

Most cyber attacks succeed not because they are clever, but because basic controls are missing.

Cyber Essentials gives every organisation a practical, government-backed way to close those gaps. Cyber Essentials Plus adds independent proof that the controls are working. Together, they form the foundation for a mature, resilient approach to cyber security, and a trusted signal to everyone you work with.

Start Your Cyber Essentials Journey

Speak with one of our IASME-qualified assessors.

Find the right level of certification for your organisation, with expert support from first questions to renewal.

Cyber Essentials from £320 + VAT

Cyber Essentials Plus from £1,395 + VAT

cyberlab.co.uk/ce



Protecting the nation, business and people.

CyberLab is a CREST-, CHECK- and NCSC-accredited cyber consultancy and managed service provider, trusted by 1,200+ organisations.

With 30+ years of expertise, we deliver expert-led penetration testing, compliance, and strategic support. We've successfully delivered 1,500 Cyber Essentials and Cyber Essentials Plus certificates, reducing risk and building resilience through a truly consultative approach.

Protecting the nation, business and people.

Speak With an Expert

hello@cyberlab.co.uk | cyberlab.co.uk

Awards and Accreditations



intertek





cyberlab

cyberlab.co.uk