

**SECURE**  
STEP FORWARD

# Cyber Essentials Checklist: What You Need to Pass

# Introduction

## Why Cyber Essentials Matters

You don't need to be a cybersecurity expert to understand that customers, partners, and suppliers **expect your business to protect sensitive information**. One simple mistake can lead to big consequences, from data breaches to lost trust.

That's where **Cyber Essentials** comes in. It's a government-backed certification that proves your business takes cyber threats seriously and it helps you win more business along the way.

This guide breaks down what Cyber Essentials involves, what's required to pass, and how to get started. **No jargon. No stress.** Just practical steps to help you protect your business and show the world you mean it.



## What Is Cyber Essentials?

Cyber Essentials is a certification that helps businesses protect themselves from the most common cyber attacks, things like phishing, malware, and unauthorised access. It's designed to make sure you've got the right basic controls in place to keep your systems and data safe.

If you're aiming to **grow, bid on government contracts, or just reassure your clients** that you take cybersecurity seriously, Cyber Essentials is a smart step forward.



### Who Should Consider It?



Businesses handling sensitive or regulated data



Organisations wanting to differentiate from competitors with verified security



Companies bidding on government, NHS, or MoD contracts



Any business looking to move beyond the basics and show they're serious about security

Cyber Essentials is ideal for any organisation that wants to demonstrate basic cyber hygiene, especially small to medium-sized businesses looking to build trust, reduce risk, and meet supplier or government requirements.

# The Five Key Areas You'll Be Assessed On

## The Simple Breakdown

To pass Cyber Essentials, your business needs to show that you've implemented key security measures in **these five areas**:

### + Firewalls

- You must use boundary firewalls to secure internet connections and block unauthorised access.
- Your firewall must be properly configured and up to date.

### + Secure Configuration

- Default settings on software, devices, and systems should be reviewed and changed to improve security.
- Remove or disable unnecessary functions and accounts.

### + User Access Control

- Make sure only the right people have access to your systems.
- Use strong passwords and restrict admin rights to those who genuinely need them.

### + Malware Protection

- Install anti-malware software or use application whitelisting to prevent malicious software from running.
- Keep your antivirus tools active and up to date.

### + Security Update Management

- Keep all software and devices updated with the latest security patches.
- Set updates to install automatically where possible.

## Why Get Certified?

- **Win more contracts**, many government and private sector opportunities require it
- **Build trust** with customers and partners
- **Protect your data and systems** from everyday cyber threats
- **Lower your risk** and potentially save on cyber liability insurance
- **Strengthen your security culture** across the whole business



# Myths About Cyber Essentials

Let's Clear These Up

“It's only for big businesses.”

Wrong! Cyber Essentials is designed for organisations of all sizes, especially SMEs that want to protect themselves and grow with confidence.

“We already have antivirus - that's enough.”

Antivirus is just one part of the puzzle. Cyber Essentials covers a broader set of risks and shows that your whole setup is secure, not just one piece of it.

“It sounds complicated and expensive.”

It doesn't have to be. We work with businesses of all sizes and tailor the process to your needs and budget. And we explain everything clearly, no tech talk needed.

## What's The Process Like?

We refer you to our trusted Certified Essentials Certifying Body, Pentest People. Their team of experts will then follow the process below:

- + Review your setup and identify any gaps
- + You implement the five key controls (with help if you need it)
- + You complete a simple self-assessment
- + Guide you through certification and support you at every step

# What Is Cyber Essentials Plus?

Taking Your Security a Step Further

Think of Cyber Essentials Plus as the premium version of Cyber Essentials. It includes everything in the basic certification plus a hands-on technical audit carried out by a qualified assessor.



Instead of simply saying you meet the requirements, Cyber Essentials Plus proves it with real-world testing. This includes vulnerability scans, configuration checks, and simulated attacks to ensure your security measures actually work in practice.

If your business handles sensitive data, operates in a regulated industry, or wants to give clients total confidence in your defences, **Cyber Essentials Plus is the clear next step.**

## What the Audit Includes

- External vulnerability scan to check for public-facing weaknesses
- Internal assessment of desktops, laptops, and other devices
- Email and browser testing to spot common phishing and malware risks
- Verification of patching and anti-malware controls
- Evidence-based review of your secure configuration and access controls

## Why Upgrade to CE Plus?

- Greater assurance - independent, expert verification of your defences
- Meets stricter contract requirements (including many public sector and MOD contracts)
- Identify weaknesses you might not spot on your own
- Reinforce customer trust with evidence-based security credentials
- Boost your readiness for more advanced compliance frameworks (like ISO 27001)

## Next Steps: Let's Talk

Thinking about getting Cyber Essentials certified?

We'd love to walk you through what's involved and help you get started.