SHORT GUIDE

everythingtech
@everythingtechgroup

Cyber Essentials 2026: What Every Business Must Prepare For

A Practical Guide to Reducing Risk, Protecting Clients & Enhancing Compliance

Concerned About Compliance Risks or Cybersecurity Threats? Contact us Today

hello@everythingtech.co.uk | www.everythingtech.co.uk | 0161 826 2220

everythingtech
@everythingtechgroup

Cyber Essentials 2026: What Every Business Must Prepare For

This guide is for IT managers and business leaders responsible for cyber security, compliance, or Cyber Essentials.

About This Guide

With cyber attacks becoming more frequent and increasingly targeted at organisations of all sizes, this guide provides an accessible, action-oriented pathway to:

- Understand the importance of Cyber Essentials in today's risk landscape
- Recognise how Cyber Essentials helps reduce exposure to common cyber attacks
- Assess your organisation's readiness using clear, structured checkpoints
- Strengthen cyber security not only internally, but across your entire supply chain
- Build confidence that your organisation, and those you rely on, meet recognised, government-endorsed security standards

Guide Contents

Whether you are just beginning your Cyber Essentials journey or looking to align suppliers to stronger cyber expectations, this guide gives you the essential context and the practical steps needed to act with confidence.

New 2026 Cyber Expectations

The Cyber Security & Resilience Bill & NCSC Priorities

2026 brings tougher cyber demands for organisations. The Cyber Security & Resilience Bill, alongside the NCSC’s stronger push on Cyber Essentials, means businesses must be able to demonstrate that they can protect sensitive data and operate securely.

Key impacts for organisations include:

- Greater expectations around safeguarding sensitive data, financial information, and personal records
- Increased scrutiny of software providers and third-party suppliers that handle data or deliver critical services
- Cyber Essentials increasingly viewed as the minimum baseline for demonstrating good cyber hygiene
- Growing pressure from clients, regulators, partners, and insurers to evidence cyber resilience and operational security

In short: Cyber Essentials is increasingly expected of any credible, modern organisation.

The Cyber Security & Resilience Bill

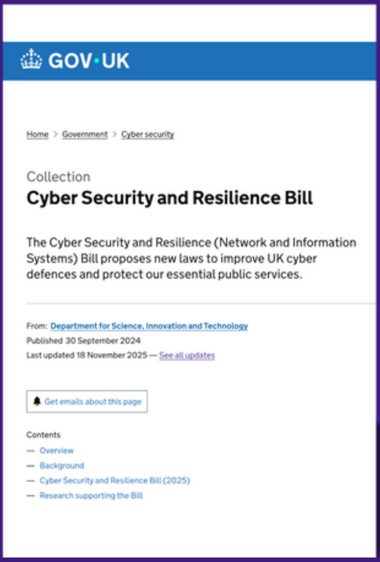
The 2026 Bill will tighten cyber rules for UK organisations:

What’s changing

- Leadership held directly accountable
- Mandatory incident reporting
- MSPs regulated
- Tougher supply-chain security
- Stronger enforcement and penalties

Why it matters

- Your organisation likely handles high-risk data
- Insurers/regulators expect evidence of controls
- Downtime impacts deadlines + client trust
- Your MSP’s compliance affects yours



GOV.UK

Home > Government > Cyber security

Collection
Cyber Security and Resilience Bill

The Cyber Security and Resilience (Network and Information Systems) Bill proposes new laws to improve UK cyber defences and protect our essential public services.

From: Department for Science, Innovation and Technology
Published 30 September 2024
Last updated 18 November 2025 — See all updates

Contents
— Overview
— Background
— Cyber Security and Resilience Bill (2025)
— Research supporting the Bill

everythingtech
@everythingtechgroup

How Cyber Essentials can help secure your business

AA simple, proven framework to safeguard your data and critical systems

Almost half (43%) of all UK businesses suffered a cyber attack over the last year.

In today's digital world, cyber attacks are inevitable, and the consequences can be costly. That's where Cyber Essentials comes in.

- Cyber Essentials is a UK government-backed certification that demonstrates that your organisation has implemented the essential security controls that protect against most common cyber threats. It is the minimum standard of security that the NCSC would advise every organisation to achieve.
- The scheme is delivered by the NCSC - in partnership with DSIT - through the IASME Consortium, who manage a network of over 400 Cyber Essentials Certification Bodies.
- Implementing just five key controls **reduces risk, strengthens resilience, and gives stakeholders verified assurance** that your organisation prioritises cyber security and meets recognised baseline standards.

Firewalls	**Secure configuration**	**Security update management**	**User access control**	**Malware protection**

There are two levels of certification:

- Cyber Essentials: a combination of self-assessment and independent audit
- Cyber Essentials Plus: the same protections, but with rigorous, independent technical testing

At Everything Tech, we help hundreds of businesses achieve both. We always recommend Plus, because it's the difference between locking your front door yourself... and having a professional come and make sure it's actually secure!

Concerned About Compliance Risks or Cybersecurity Threats? Contact us Today

hello@everythingtech.co.uk | www.everythingtech.co.uk | 0161 826 2220

Cyber Essentials & Cyber Essentials Plus — 2026 Updates

The biggest CE/CE+ update since v3.1

From 27 April 2026, Cyber Essentials (CE) and Cyber Essentials Plus (CE+) assessments move to version 3.3, bringing several key changes that will directly affect businesses like yours.

Headline updates

- Cloud services fully in scope
- No exceptions — M365, Xero, payroll systems, document portals, identity platforms.
- Mandatory MFA for all cloud services
- If MFA exists but isn't enabled, you fail.
- New scoping rules
- Anything that touches the internet is in scope unless you can prove effective segregation.
- Updated software and web application requirements
- Relevant for custom portals and internal apps.
- Passwordless authentication encouraged
- Expect a shift away from traditional password policies.
- Backups prioritised earlier in the standard
- Backup processes must be documented, tested and auditable.

Why CE matters more than ever for businesses

1. Insurers now expect it

Many cyber insurers view CE as the minimum baseline, some policies require it.

2. It reduces operational risk

Helping ensure systems remain secure and available during critical business operations and high-impact moments.

3. It strengthens customer and partner assurance

More clients, customers, and partners now request Cyber Essentials or Cyber Essentials Plus as part of due diligence.

4. Attackers target businesses your size

Mid-sized organisations are especially vulnerable, they often hold high-value data without enterprise-grade security controls.

Cyber Essentials Made Simple: A Handy 4-step Plan for Businesses

1. Secure Your Own Practice First

- Get your business Cyber Essentials-ready by implementing the five core controls. If you expect suppliers to meet a standard, your organisation should meet it too.

2. Understand Your Risks & Identify Key Suppliers

- Map where sensitive data flows, which systems are business-critical, and which third-party suppliers present the highest risk.

3. Set Clear Cyber Essentials Requirements

- Decide which suppliers need CE or CE Plus, add these expectations into onboarding, contracts, and renewals, and explain why it matters.

4. Embed, Support & Monitor Adoption

- Give suppliers guidance, track their certification, build CE into procurement processes, and review compliance annually.

How Everything Tech Helps Businesses Stay Secure & Compliant

At Everything Tech, we specialise in helping businesses strengthen their cyber security, streamline their IT, and meet modern compliance expectations. Our services combine proactive IT support, robust security management, and compliance-ready solutions built specifically with frameworks like Cyber Essentials and Cyber Essentials Plus in mind.

Cyber Essentials & CE Plus Made Simple

We guide organisations through the entire Cyber Essentials journey: identifying gaps, fixing issues, preparing evidence, and supporting the independent CE Plus audit. We make the process smooth, predictable, and stress-free, whether you're certifying for the first time or renewing.

Proactive IT Support & Security That Scales With Your Business

We support growing organisations with IT that keeps teams productive and secure, combining rapid remote response with regular onsite support. From phishing protection and device hardening to compliance guidance and hybrid-working optimisation, we help organisations streamline operations, reduce risk, and stay ahead of evolving threats. The result? Faster onboarding, stronger cyber hygiene, smoother system upgrades, and teams free to focus on what they do best.

What Next?

The guidance in this document is a starting point, not a full compliance guarantee, but preparing early puts your business in a much stronger position.

Reach out to our team, and we'll review your current security posture, including Cyber Essentials. We'll provide tailored advice, a long-term security roadmap, and ongoing recommendations to help your business stay compliant and protected.

> *As an organisation, we're incredibly happy with Everything Tech's proactive approach to security.*

everythingtech
everythingtechgroup

Concerned About Compliance Risks or Cybersecurity Threats? Contact us Today

hello@everythingtech.co.uk | www.everythingtech.co.uk | 0161 826 2220