Cyber Essentials and Cyber Essentials Plus

What is Cyber Essentials and Cyber Essentials Plus?

It is a cost-effective baseline cyber security certification. Considered the best first step to a more secure network and once implemented protects you from over 95% of the most basic cyber security breaches.

It is a UK Government backed scheme that covers the essentials steps every business should take whatever its size to protect itself from cyber threats.

Cyber-attacks come in many shapes and sizes and are the digital equivalent of a thief trying your front door to see if it's unlocked. This certification is designed to prevent these attacks.

The certification has become an essential tool for safeguarding sensitive information, preventing data breaches, protecting against malicious attacks, and maintaining business continuity.

The rise of consumer awareness of the impacts of cyber-attacks or the consequences of personal data breaches, have rightly seen an increased demand for evidence that your business takes its responsibilities seriously and invests in cyber protection.

This certification covers 5 key criteria:

1. Is your internet connection secure?
2. Are the most secure settings switched on for every company device?
3. Do you have full control over who is accessing your data and services?
4. Do you have proper protection against viruses and malware?
5. Are your devices and software updated with the latest versions?

What are the 5 Controls of Cyber Essentials?

1. Firewalls
2. Secure configuration
3. Security Update Management
4. User Access Controls
5. Malware Protection

Two levels of certification

Cyber Essentials

This is an independently verified self-assessment certification that demonstrates that an organization has the most important cyber security controls in place. It provides you with the peace of mind that your defences will protect against the most common cyber-attacks. Cyber Essentials shows you how to address these basics and prevent the most common attacks. The certification is annually renewable.

Cyber Essentials Plus

This assessment aims to confirm that all technical controls that have been declared on the Cyber Essentials are correct and are implemented on the organization network. Highly trained assessors carry out vulnerability tests to make sure that your organization is protected against basic hacking and phishing attacks.

The Cyber Breaches Survey, conducted annually by the Department for Science, Innovation and Technology (DSIT) reported in March 2023 that around a third of businesses and a quarter of charities had experienced a cyber attack in the previous 12 months. The larger the organisation the more likely they were to have experienced an incident: 69% of large firms and 76% of charities with annual incomes over £5 million reported breaches.

Cyber Breaches Survey Report

Benefits of achieving certification

Improve your Security processes

Certification to Cyber Essentials is a great first step towards GDPR compliance and one that is being recognised by the Information Commissioners Office as good practice. Cyber Essentials can mitigate penalties should an organisation suffer a breach.

Build trust with customers

Having a government-backed accreditation lets customers know that you operate your business to a good standard of cybersecurity. This provides the reassurance they need to buy from you with confidence. Over time, you'll build broader brand recognition and improve your reputation, too.

Bid for Government contracts

If you want to work with organisations in the public sector and bid for contracts, you'll need a Cyber Essentials accreditation.

This is a huge opportunity to work on large-scale projects and form long-lasting positive relationships with public sector organisations.

Be on a trusted register of suppliers

For the 12 months your certificate is valid, your company's name will be on the NCSC & IASME website. This makes it easy for potential customers to check your cybersecurity credentials and validate your business.

Cyber Liability Insurance

Cyber Essentials certification includes automatic cyber liability insurance for any UK organization that certifies their whole organization and has less than £20m annual turnover.

Strengthen your supply chain

It's not just important for your customers to trust you. Your partners, suppliers, and investors need to have confidence in your ability to operate safely, too. Having a recognised certification validates your processes and means they know you operate with their best interests at heart.

Reassurance

It provides you with peace of mind that your defences will protect against the vast majority of common cyber attacks.

We estimate that, across all UK businesses, there were approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud in the last 12 months.

Cyber Breaches Survey Report

Cyber Essentials vs ISO 27001

Cyber Essentials and Cyber Essentials Plus focuses on fundamental IT controls to ensure they are robust and resilient to cyberattacks, whereas ISO 27001 takes a more holistic approach incorporating policies and procedures.

We recommend achieving both Cyber Essentials & Cyber Essentials Plus in addition to ISO 27001 as it demonstrates your commitment to good security practices. Becoming certified in both is a sensible option for ensuring robust protection on both the Information security side as well as Cyber Security.

What are the differences between ISO 27001 and Cyber Essentials?

Whilst Cyber Essentials and ISO 27001 are both technical standards aimed at organizations wishing to demonstrate compliance, each standard has some key fundamental differences as outlined below:

Why BSI

For over 100 years, BSI have driven best practice in business around the world. With more than 90 offices in 30 countries we reach over 86,000 clients, supporting them to develop a resilient organization.

We bring together the collective wisdom of over 11,000 experts to generate best practice for business. Assessment services with BSI or via our partners of excellence provide reassurance that you're robust and committed to business improvement and best practice as well as delivering value to your stakeholders.

Get in touch today and find out more

Call: +44 (0)345 0765 606
Email: product.certification@bsigroup.com
Visit: bsigroup.com/iot

	Cyber Essential Plus	ISO 27001
Region	UK Only	International standard
Type of standard	Technical, compliance-based standard	Risk-based standard
Definition	Based on a set of 5 common themes covering the most common Internet-originated attacks against an organization's IT systems and services. • Firewalls • Secure Configuration • User Access Control • Malware Protection • Security Update Management	Defines requirements for the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS). ISO 27002 guides the implementation of 93 best practice safeguards organized in 4 domains: • Organizational • People • Physical • Technical
Business size	Organizations of any size	Organizations of any size
Applicability	Scope limited to digital areas	The scope encompasses physical and digital assets
Scope	All controls required for certification	Safeguards are applied based on the type of business activities undertaken
Contractual	Mandatory for UK Government and MOD contracts	Implementation and certification are optional
Frequency	Annual renewal	Typically, 3 years with annual audits