Cyber Essentials Guide

Earn your Cyber Essentials accreditation and demonstrate you are serious about security.

About this guide

This guide tells you everything you need to know about Cyber Essentials – from what it is; how to get accredited; and how it will benefit your business.

Introduction

What is Cyber Essentials?........3–4

Why is Cyber Essentials Important?........5

Accreditation 101........6

How can the Cyber Essentials toolkit help?........7

What is Cyber Essentials?

Cyber Essentials is an effective UK Government scheme that focuses on the five technical controls designed to guard against the most common internet-based cybersecurity threats:

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

Cyber Essentials is now widely recognised as the minimum baseline level of cybersecurity for organisations of all sizes.

Cyber Essentials certification includes automatic cyber liability insurance for any UK organisation that certifies its whole organisation and has an annual turnover of less than £20 million (terms apply).

39%

39% UK businesses reported suffering a cyberattack in 2022

The Latest Cybercrime Statistics (updated April 2023)[1]

54%

54% businesses actively identify cybersecurity threats

Cyber Security Breaches Survey 2022[2]

87%

87% small businesses have customer data that could be compromised

51% of Small Businesses Admit to Leaving Customer Data Insecure, Digital.com[3]

There are two levels of certification:

CYBER ESSENTIALS

This self-assessment option gives protection against a wide variety of the most common cyberattacks and makes a business less vulnerable to more in-depth unwanted attention from cyber criminals and others. The accreditation is designed to educate on the best practices surrounding cybersecurity and minimise the risk of being identified as a potential target by bad actors.

Gaining the Cyber Essentials certification will prove to your clients that the defences you have in place are robust and will protect them against the most common attacks. Cybercriminals will often look for easy targets, rather than businesses with the Cyber Essentials technical controls in place.

CYBER ESSENTIALS PLUS

Cyber Essentials Plus shares the Cyber Essentials trademark simplicity of approach and puts the same levels of protection in place. However, with Cyber Essentials Plus a hands-on technical verification is carried out by a qualified assessor.

The audit includes an internal and external vulnerability scan and then focuses on a selection of user devices, all internet gateways and all servers that are accessible to internet users.

The third-party assessment offered by Cyber Essentials Plus offers your clients additional peace of mind that your business has been independently recognised as secure, with robust protective measures in place.

Why is Cyber Essentials important?

The finer details

Cyberattacks come in many shapes and sizes, but they're becoming increasingly complex and harder to spot. Businesses must constantly build on their cybersecurity measures to keep ahead of the bad actors looking to profit from their hard work.

Basic cybersecurity is essential for all organisations and their supply chains. Cyber Essentials is a UK Government backed scheme that helps MSPs safeguard their organisation, and their clients, against most common internet threats.

The Cyber Essentials certification badge signals to customers, investors and suppliers that an organisation has put the Government approved minimum level of cybersecurity in place and can be trusted with their data and business. With cyberattacks becoming an increasing threat, SMBs must prove to their prospects and clients that it's safe to do business with them. Cyber Essentials is designed to do precisely that.

What role does IASME play?

On 1 April 2020, IASME (Information Assurance for Small and Medium Enterprises) became the National Cyber Security Centre's sole Cyber Essentials Partner, responsible for the delivery of the scheme.

IASME works alongside a network of over 300 expert organisations across the UK and Crown Dependencies to help advise and certify organisations of all sizes in both cybersecurity and counter fraud. IASME is committed to helping businesses improve their cybersecurity, risk management and good governance through an effective and accessible range of certifications.

Accreditation 101

How will the accreditation benefit your business

Certification gives you peace of mind that your defences will protect against the vast majority of common cyberattacks and demonstrates your commitment to cybersecurity.

Cyber Essentials will:

- Reassure customers that you are working to secure your IT against cyberattack.
- Attract new business with the promise that you have cybersecurity measures in place.
- Give a clear picture of your organisation's cybersecurity level.
- Grow business as some Government contracts require Cyber Essentials certification.

Remember to renew your certification annually as it expires after 12 months. Companies will be removed from IASME's list of certified organisations if they are not certified within twelve months of their last certificate.

Cyber Essentials certification also includes automatic cyber liability insurance for any UK organisation that certifies its whole organisation and has an annual turnover of less than £20 million (terms apply).

What does the cyber liability insurance cover?

- Liability – claims made against you stemming from media activities, and privacy or security wrongful practices.
- Crisis management – emergency costs following a data breach (including the costs of notifying data subjects).
- Regulatory investigations – defence costs and regulatory fines (where insurable by law).
- Business interruption – loss of profit, or operational expenses caused by a network compromise.
- Loss of electronic data – costs of remedying the issue that enabled the loss or damage of your data.

How do businesses get accredited?

MSPs who want to gain Cyber Essentials accreditation will need to assess themselves and provide evidence against the five basic security controls: firewalls, secure configuration, user access control, malware protection, and security update management.

The Cyber Essentials self-assessments are available through a secure hosted platform powered by the Cyber Essentials assessment platform.

Find Out More

How can the Cyber Essentials Readiness Tool help?

The Cyber Essentials Readiness Tool is a free interactive website developed by IASME, on behalf of the National Cyber Security Centre, that helps organisation's look at their cybersecurity. As you work through a questionnaire, you will be able to gauge your current level of cybersecurity in relation to where you need to be to achieve Cyber Essentials.

Many MSP businesses know they need to take control of their cybersecurity, but don't know where to start. The Readiness Tool is the first step in the journey towards becoming Cyber Essentials certified. It is designed to support and educate, shedding light on some of the technical terms and creating a tailored pathway to follow.

To use the tool, follow these simple steps:

- Go online to the Cyber Essentials Readiness Tool
- Work your way through a series of questions that address different elements of your organisation's security.
- Throughout the questionnaire, there are additional guidance documents available to help you understand the five technical controls and how they relate to your business.
- Your answers will form the basis of a step-by-step action plan that will be presented to you when you reach the end of the readiness tool.
- Download or print off your readiness action plan and start to work your way through the actions.

All the self-assessment questions are available to download for free in advance.

Want to learn more about how to acheive the Cyber Essentials accreditation?

Pax8 is here to help

Schedule a Call

Sources

1. https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=39%25%20of%20UK%20businesses%20reported,of%20%C2%A34200%20in%202022.
2. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
3. https://digital.com/51-of-small-business-admit-to-leaving-customer-data-unsecure/#:~:text=87%25%20of%20small%20businesses%20have%20customer%20data%20that%20could%20be%20compromised

pax8.com | info@pax8.co.uk