CyberSmart

2022 EDITION

A guide to cybersecurity certifications in the UK

From Cyber Essentials to ISO 27001

cybersmart.co.uk

Contents

INTRODUCTION

The journey to a safer, more productive business

Ever since the Cyber Essentials scheme launched in 2014, companies have used it, and similar cybersecurity certifications, to showcase their trustworthiness and meet industry regulations. Conscientious companies that complete such schemes get listed on a searchable register of certified businesses and organisations.

But the truth is that the journey to cybersecurity compliance isn't as simple as filling out an application. The route can wind from the basics of Cyber Essentials to the independent auditing of Cyber Essentials Plus. Some organisations even choose to tackle the challenge of ISO 27001 compliance.

In this guide, we cut through the noise and outline the three most common UK cybersecurity certifications, how to choose the right one for you, and how to get certified.

Cyber Essentials

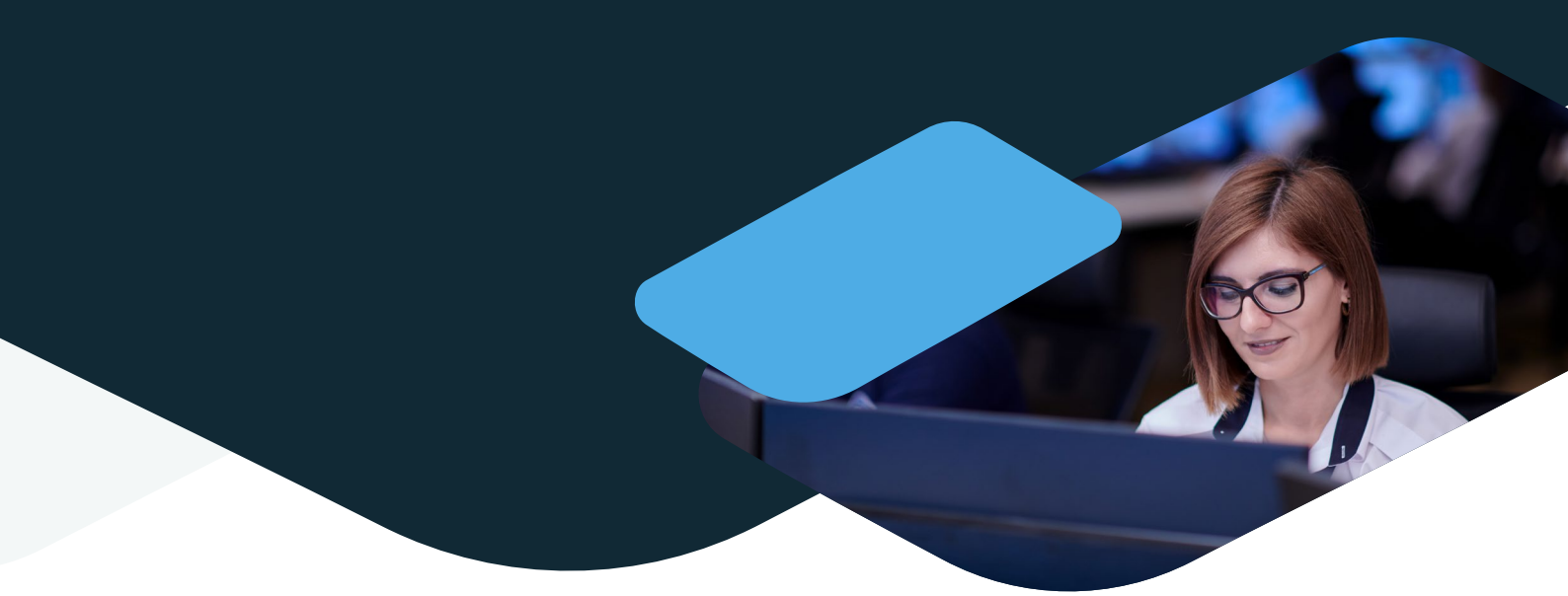
- **Good for:** Any business
- **Key features:** Self-assessment, accessible to all businesses
- **Certification requirements:** Basic

Cyber Essentials Plus

- **Good for:** Actively growing businesses, industries with higher security requirements
- **Key features:** On-site technical audit
- **Certification requirements:** Detailed

ISO 27001

- **Good for:** Highly-regulated industries
- **Key features:** Processes and policies, internal and external audits
- **Certification requirements:** In-depth



CYBER ESSENTIALS

CYBER ESSENTIALS

The first port of call

The Cyber Essentials scheme is a UK cybersecurity certification that outlines the security procedures a company should have in place to secure their data. Cyber Essentials is highly recommended for SMEs because this certification protects you against 98.5% of the most common cyber threats.

This certification covers:

- Firewalls
- Internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management

How Cyber Essentials works

To achieve a Cyber Essentials certification, you must complete a self-assessment questionnaire and submit it through an online portal. Once you've applied, a certification body assesses and grades the application.

Sample Cyber Essentials certification questions

- **A2.5.** Please list the quantity of servers, virtual servers, and virtual server hosts (hypervisor). You must include the operating system. Please list the quantity of all servers within scope of this assessment.
  For example: 2 x VMware ESXI 6.7 hosting 8 virtual windows 2016 servers; 1 x MS Server 2019; 1 x Redhat Enterprise Linux 8.3
- **A4.7.** Have you configured your boundary firewalls so that they block all other services from being advertised to the internet?
  By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.
- **A5.10.** When a device requires a user to be present, do you set up a locking mechanism on your devices to access the software and services installed?
  Device locking mechanisms such as biometric, password, or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.

And that's really all there is to it. Once certified, your accreditation is valid for 12 months. After 12 months, you must reapply for the certification.

We recommend Cyber Essentials if...

- **...you're an SME that wants to protect its digital assets from cybercrime**
- **...you're looking to achieve certification to get on the public register**
- **...you want to win new business by displaying your cyber credentials**

But, if you want to show your clients that you have robust cybersecurity procedures, you need verification from an independent expert. For that, you need Cyber Essentials Plus.

Cyber Essentials Evendine Update: 24th Jan 2022

The cybersecurity landscape has changed so much since 2014. So, to help you tackle today's cybersecurity challenges, IASME and the NCSC updated the requirements of the Cyber Essentials certification. The new Cyber Essentials update – known as Evendine – launched on January 24, 2022.

The update includes new requirements and clarification for:

Cloud services

Multi-factor authentication

Working from home

Software and licences

Cloud services

If an organisation's hosts data or services on a cloud service, the organisation is responsible for implementing Cyber Essential controls. Definitions of cloud services have been added for:

- Infrastructure-as-a-Service (IaaS)
- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS)

ISP-provided routers are now out of scope and don't need to be listed, but organisation-owned routers do.

Multi-factor authentication

Multi-factor authentication provides additional protection to administrator accounts when connecting to cloud services. Multi-factor passwords must contain at least 8 characters with no maximum length restrictions.

Working from home

Any devices that home workers use to access organisational information are in scope for Cyber Essentials. Corporate VPNs transfer the boundary to the corporate firewall or virtual cloud firewall. Thin clients come into scope when they connect to company information or services.

All smartphones and tablets that connect to a corporate network to access data and services are in scope when connecting via mobile internet (4G or 5G). Users must lock them with biometrics or a minimum password or PIN length of 6 characters.

Software and licences

All software on in scope devices must be:

- Licensed and supported
- Removed from devices when it becomes un-supported
- Removed from scope by using a defined ‘sub-set’ that prevents traffic to and from the internet
- Enabled to update automatically where possible
- Updated, including applying any manual configurations, within 14 days of a new update

Separate user accounts to perform administrative activities only. This means that the account is separate from avoidable risks, such as emailing, web browsing, and similar activities.

CYBER ESSENTIALS PLUS

CYBER ESSENTIALS PLUS

The next step

Cyber Essentials Plus has the same simple approach as Cyber Essentials but includes a technical audit of your systems. The controls you need are the same – the audit just makes sure they're in place.

The audit element of the Cyber Essentials Plus certification requires some more effort, but it offers you the peace of mind that your new protections work effectively.

How Cyber Essentials Plus works

- The online assessment is the same as the Cyber Essentials Plus certification
- If you have Cyber Essentials already, you must make your Plus audits within 3 months of your last certification
    - New applicants can complete their online certification as part of Cyber Essentials Plus
- Auditors typically review your head office and some of your other offices to carry out the tests on a random sample of your systems
- Many auditors offer remote audits
- Accredited businesses are certified for 12 months

We recommend Cyber Essentials Plus if...

- ...you want a thorough assessment of your cybersecurity measures, plus a certification.
- ...you work with (or want to work with) high-quality clients and want to show them that data protection is a top priority
- ...you work in an industry with higher-than-standard cybersecurity requirements

Businesses with a cybersecurity certification can win more business, making certification a valuable commodity in competitive markets. By showing your commitment to cybersecurity, you can build trust with new customers.

For businesses with the budget and ambition to take their accreditations further, we recommend ISO 27001.

ISO 27001

A new frontier

ISO 27001 is the leading international standard for information security. Over 44,000 organisations all over the world use ISO 27001 to protect their data. The basic goal of the certification is to protect three aspects of information:

- **Confidentiality.** Only authorised people have the right to access information
- **Integrity**. Only authorised people can change the information
- **Availability.** The information must be accessible to authorised people whenever it's needed

Successful implementation of ISO 27001 requires careful planning and project management. Unlike the checklist-style of Cyber Essentials, ISO 27001 is an interlocking framework of policies and processes. So, you'll need to create process documents and maintain mandatory records of training, internal audits, and more.

How ISO 27001 works

- Before inviting an auditor, perform a gap analysis to identify the status of information security, and an initial expectation of required effort
- Produce the relevant documents and processes
- Invite the auditor to assess your efforts
- Accredited businesses are certified for 3 years. During this time, the certification body performs surveillance audits to check in on your activity

We recommend ISO 27001 if...

- **...your business specifically needs an ISO 27001 certification**
- **...your customers and competitors also have ISO 27001**
- **...you work in the health or public sectors**

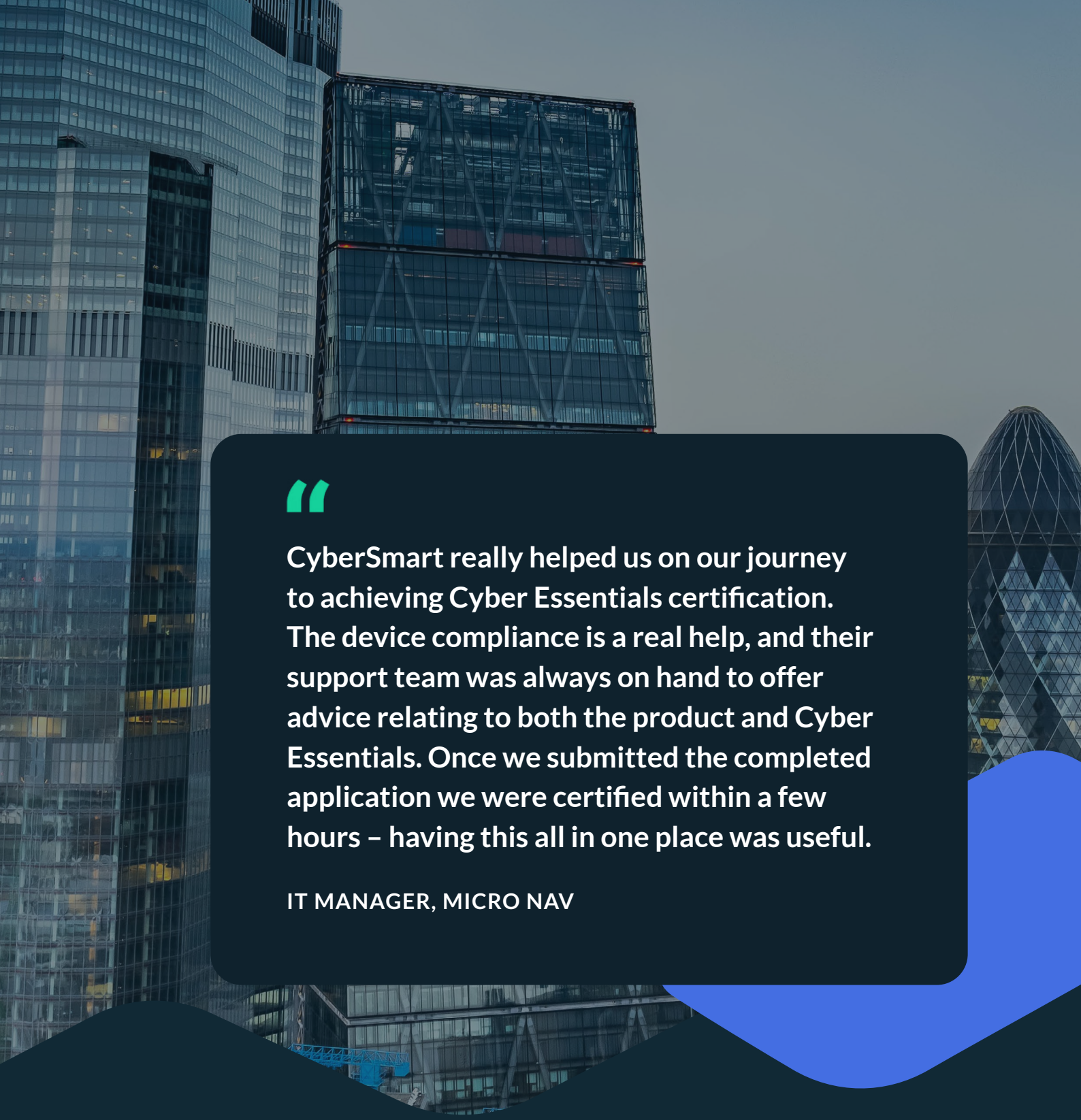
COMPLIANCE MADE EASY

How to take your cybersecurity certifications further

The best way to go the 360˚ protection route is to choose one certification to implement first and then transition to the other. Don't make the mistake of trying to do everything at once!

If you want to cover all bases, you can work towards both the ISO 27001 and Cyber Essentials. Just because you're ISO 27001 certified, it doesn't mean that you're Cyber Essentials compliant or vice versa. Being certified in both is an excellent way to ensure 360˚ protection, but it requires considerable investment.

For most businesses, we recommend starting with Cyber Essentials because it's a self-serve option, making it a simple way to start your cybersecurity journey. ISO 27001 requires a bigger up-front investment because you must move from general security management procedures to documented and audited cybersecurity processes.



> CyberSmart really helped us on our journey to achieving Cyber Essentials certification. The device compliance is a real help, and their support team was always on hand to offer advice relating to both the product and Cyber Essentials. Once we submitted the completed application we were certified within a few hours – having this all in one place was useful.
>
> IT MANAGER, MICRO NAV

INDUSTRY ACCOLADES

CompTIA UK SPOTLIGHT WINNER CyberSmart INNOVATIVE VENDOR AWARD

SC 2022 awards EUROPE WINNER

Navigate cybersecurity compliance with CyberSmart

Adapting to ever-changing cybersecurity standards is both a challenge and an opportunity. The Cyber Essentials scheme is a chance to highlight your company's commitment to protecting client data. At CyberSmart, we've helped many clients achieve Cyber Essentials and Cyber Essentials Plus certifications.

We offer all the guidance you need to pass your certification – with tips and live support that mean you'll answer the questions correct first time. If your business is a bit more complex and you need to supply additional info, there's no charge for resubmissions. With CyberSmart, you can be certified in as little as 24hrs and our easy-to-use dashboard makes managing the whole process simple.

We also offer free cyber insurance covering up to £25k with certification. So, if you're ready to begin your cyber security journey, get in touch today.

Get in touch