CYBER ESSENTIALS

10 years of Cyber Essentials

A decade of helping UK organisations guard against the most common cyber threats

National Cyber Security Centre

Department for Science, Innovation & Technology

Timeline

2014

Cyber Essentials launched in June 2014. Certification was soon required for certain UK government contracts, to handle sensitive and personal information

2016

Two years in, and the NCSC is formed. The scheme now has 129 licensed Certification Bodies

2019

By 2019 over 15,000 Cyber Essentials certificates are being awarded annually

2021

Cyber Essentials Readiness Tool launched; an interactive tool to help users create a personal action plan to meet the Cyber Essentials requirements

2020

IASME is appointed as the sole Cyber Essentials Delivery Partner, replacing the existing five partner model

2022

With over 30,000 awards this year, Cyber Essentials celebrated the 100,000th certificate in the lifetime of the scheme

2023

The Cyber Advisor scheme is launched; offering small orgs NCSC assured advice and practical help to implement the Cyber Essentials controls

2024

The Cyber Essentials Knowledge Hub is launched as the scheme marks it first decade

Introduction

Over 10 years ago, GCHQ was challenged by industry to identify the controls that really mattered when it came to cyber security. That was, in essence, the genesis of our journey to Cyber Essentials.

Today, as we celebrate the 10th anniversary of the Cyber Essentials scheme, I still believe it is one of the best tools available to protect the majority of organisations from the majority of cyber attacks. And, increasingly, we are finding the evidence to back that up.

Cyber Essentials not only makes organisations more resilient, but it has created an ecosystem of over 350 companies across the UK, offering quality assessment and advisory services; employing and upskilling the next generations of cyber security professionals. For that, I believe Cyber Essentials is pretty unique.

When the challenge to identify the controls that really mattered was first laid down, we had been investigating attacks against several large organisations. While we judged that each had been penetrated by a capable actor, the techniques used were far from cutting edge. Our analysis showed that one or more of just 5 key controls would have stopped the attacks progressing.

But we needed to verify that to ensure we had identified the controls that protect against an attack from the internet, using publicly known tools – a scenario that was ultimately adopted as the threat model for Cyber Essentials.

We worked with the likes of IASME and the Internet Security Foundation to get a broader community view. Many additional controls were suggested, and in each case, we assessed whether they would make a tangible difference to an organisation's security, given the threat model. We also recognised the more controls that were added, the harder and more expensive it would be for organisations.

We ended up sticking with those five controls, and the evidence we have today tells us it was a good decision. For example, companies with the Cyber Essentials controls in place are 92% less likely to make a claim on cyber insurance than organisations without.

But how could organisations demonstrate they had implemented them right? Existing security assessments at the time could be prohibitively expensive and we wanted this to have broad appeal. Self-assessment with independent validation was seen as the best approach, as it could be offered at a fixed price. But there were situations where more confidence was needed, and independent testing was included. Together they provide options matched to security needs and budgets. With this, Cyber Essentials was born.

Today Cyber Essentials continues to thrive and grow, not just as a way of improving an organisation's security, but an ideal tool to get confidence in the security of their suppliers' systems too. It's been a privilege to be part of the journey from concept to what we see today, supporting over 40K organisations to improve their cyber resilience through a national network of companies providing advice, certification, employment and upskilling. If an organisation relies on the internet in any way, Cyber Essentials is the go-to tool.

Chris Ensor, Deputy Director, National Cyber Security Centre

A minimum standard for cyber security

7.78 million cyber crimes were experienced by UK businesses over the past year. That's half of all businesses in the UK, and around a third of all charities reported a cyber security breach or attack in the last 12 months.

Of course, cyber attacks come in many different forms, but the majority are often basic in nature - the digital equivalent of a thief trying your front door to see if it's unlocked.

Cyber Essentials helps guard against the most common cyber attacks. That's why - in today's digital world, where it's more important than ever for every organisation to keep both its own and its customers' data safe and secure from unwanted attacks - Cyber Essentials is the minimum standard of security that the NCSC would recommend every organisation to achieve. And, when increased confidence is required, Cyber Essentials Plus offers an independent technical audit to verify the controls.

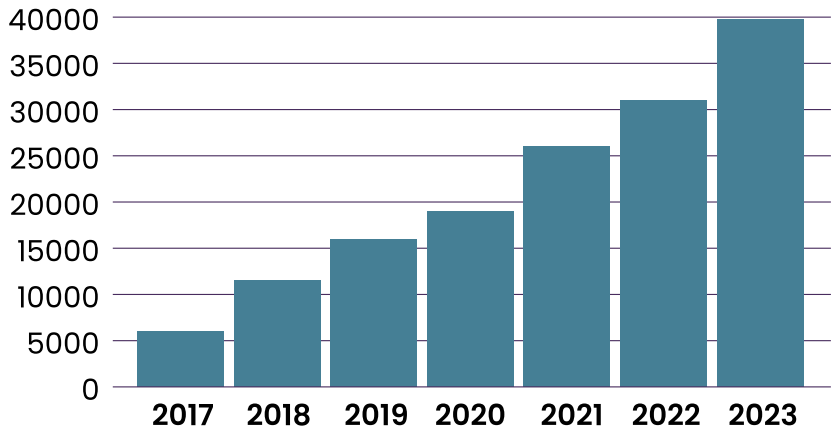
Growth of Cyber Essentials

Since its launch in June 2014, Cyber Essentials has steadily grown year-on-year in both take up and recognition.

IASME was one of multiple pilot 'Accreditation Bodies' to launch the scheme and, following a commercial tender process, took over full responsibility for Cyber Essentials delivery in April 2020.

Since IASME became the NCSC's sole Cyber Essentials Delivery Partner, the scheme has more than doubled. Between 1 September 2023 and 31 August 2024, 33,836 Cyber Essentials certifications and 10,939 Cyber Essentials Plus certifications were issued. This is a 21% increase in Cyber Essentials certificates issued and a 20% increase in Cyber Essentials Plus certificates issued since last year.

Total number of certifications (CE and CE+) issued by year



Key insights

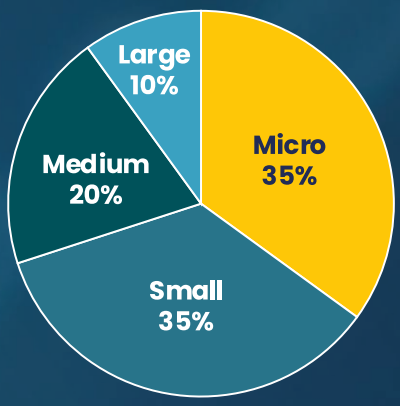
Appetite for Cyber Essentials continues to grow, with another rise in certifications awarded over the past 12 months (1 Sep 2023-31 Aug 2024)

33,836
CE certificates

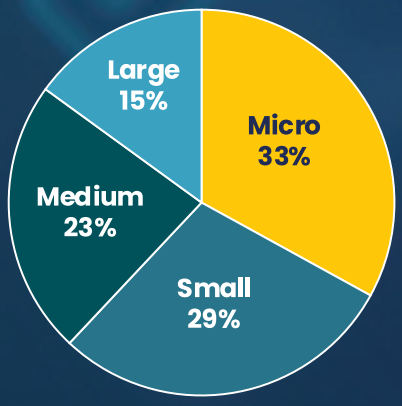
10,939
CE+ certificates

20%
Increase in certifications

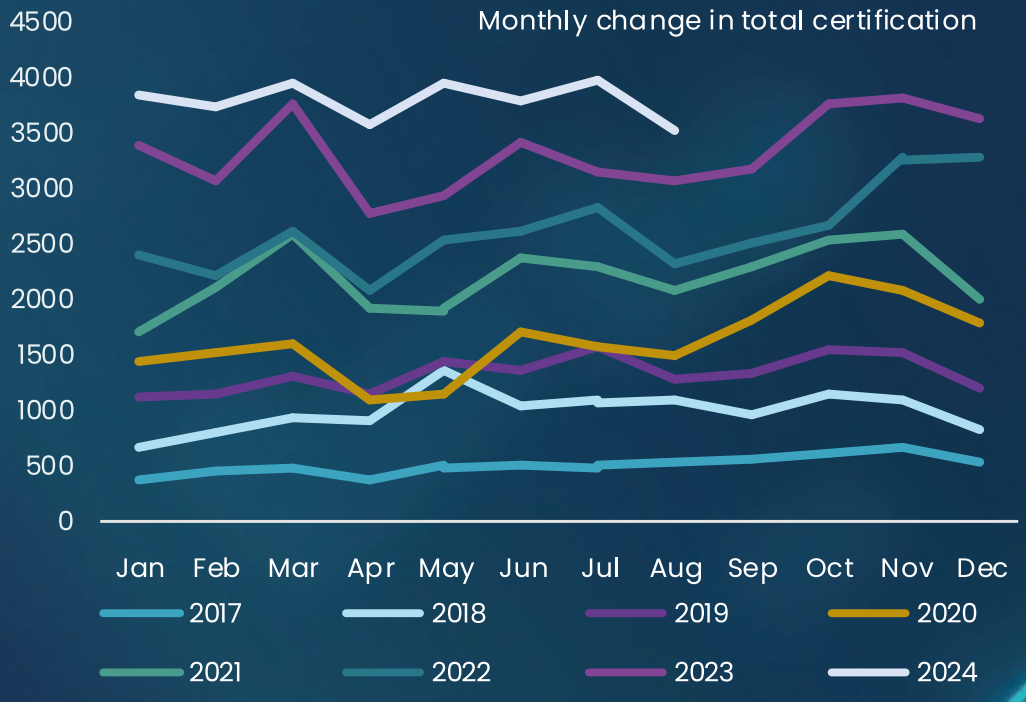
Certified Org Size - CE



Certified Org Size – CE+



Monthly change in total certification



Certification Bodies

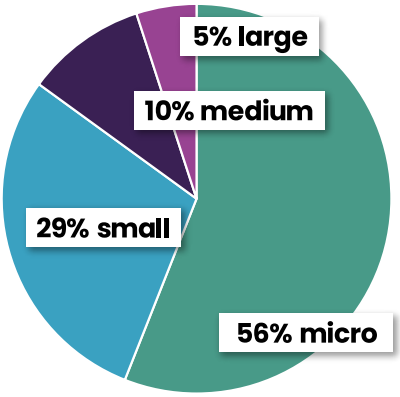
Growing the cyber ecosystem

Cyber Essentials is fuelling growth in the UK cyber security sector, with a network of over 350 Certification Bodies and almost 900 Assessors.

Through our Delivery Partner, IASME, we support the UK's cyber security industry, licensing the Cyber Essentials assessment process to trained and qualified cyber security companies called 'Certification Bodies'. Located right across the UK, these Certification Bodies assess applications, conduct audits and issue certificates.

Cyber Essentials has helped grow the cyber security industry and expertise right across the UK and Crown Dependencies. 84% of these companies are micro or small businesses, with distribution including many regions with relatively few cyber security businesses, as well as areas awaiting regeneration.

In addition, the Cyber Essentials scheme supports the growth of the Certification Bodies themselves. Some businesses have experienced significant growth, which has resulted in an increase in the number of trained cyber security experts.



358
Certification Bodies

897
Assessors employed

Cyber Advisors

Launched in April 2023, the Cyber Advisor scheme assures businesses to provide small organisations with trusted cyber security advice and practical support in implementing the Cyber Essentials controls.

There is already a network of 100 Cyber Advisors - employed by 95 different NCSC Assured providers - offering this guidance and hands-on help.

Feedback from Cyber Advisor customers has been exceptional. 100% of customers who completed a customer satisfaction survey rated the overall service provided by their Advisor as 'excellent' or 'good'.

Extending support

Since the inception of Cyber Essentials, the scheme has expanded, not just through the number of organisations achieving certification, but also in the level of support and help offered.

Over the previous page, we outlined the help available to small organisations through the Cyber Advisor scheme, which offers trusted advice and hands-on support in implementing the five technical controls set out by Cyber Essentials. But much more has also been done to help UK organisations increase their cyber resilience and achieve certification. This includes:

An alternative Pathway to certification

The Cyber Essentials technical controls have been carefully defined to protect against the most common types of cyber attack. But there are sometimes legitimate reasons why large organisations can't implement some controls. In these cases, the organisation may have other mitigations in place.

For that reason, we have been testing an alternative route to certification, when an organisation can demonstrate they have alternative technical controls which enable them to meet the overall intended outcome; that is resilience to a 'commodity attack'.

Following successful testing, the Cyber Essentials Pathways proof of concept has now been launched.

Funding small orgs in at-risk sectors

The Funded Cyber Essentials Programme aimed to help micro and small organisations protect against many of the most common cyber attacks, providing support to some of the most vulnerable small organisations in the UK, through funding and hands-on-help to gain Cyber Essentials Plus certification.

The programme has reached into charity and legal sectors and, most recently, emerging technologies companies.

To date, 525 organisations have benefitted from the opportunity to access free Cyber Essentials support.

Readiness Tool

Organisations are sometimes unsure how to prepare for Cyber Essentials. The Readiness Tool was launched by IASME in 2021 to explain the requirements and give targeted guidance on how to implement them.

The interactive tool works through a series of questions developed to lead users through the main parts of the Cyber Essentials requirements. At the end of this process, users are given tailored guidance and a list of actions outlining the steps needed to prepare for Cyber Essentials.

Recommended by Users

92%

fewer insurance claims made by orgs with Cyber Essentials controls in place

89%

would recommend certifying to Cyber Essentials to other orgs like theirs

40%

of smaller organisations implemented the controls for the first time

2%

failure rate for Cyber Essentials; dropping for the 3rd straight year

69%

of organisations with Cyber Essentials believe that it has increased their market competitiveness

88%

believe Cyber Essentials has improved their understanding of cyber security risks

91%

of customers said they would recertify to Cyber Essentials next year

80%

of organisations with Cyber Essentials believe its controls help them to mitigate cyber security risks

> “Information in the wrong hands brings significant risk... We want to show not just our commissioners we can be trusted, but also the people who come into our service. Their information is a precious commodity, and we’ve got the systems in place to protect it.”
>
> **Sara Ward, CEO, Black Country Women’s Aid**

Unaddressed risks: a supply chain threat

We have seen a significant increase in cyber attacks resulting from vulnerabilities within supply chains in recent years, including some high-profile incidents.

Despite this increasing trend, just 11% of businesses and 9% of charities review the risks posed by their immediate suppliers; with only 6% of businesses and 4% of charities reviewing the risks posed in their wider supply chains.

This may be because many organisations struggle to do this effectively. Assessing the cyber security of suppliers is seen as a challenge – many organisations consider a lack of assurance tools, insufficient expertise and a lack of visibility as significant barriers to managing supplier cyber risk.

Cyber Essentials provides a clear way to gain confidence that suppliers - or other third parties - have effectively implemented the fundamental technical controls that can protect against the majority of untargeted, commodity attacks. Requiring certification can play an important role as an assurance tool to help organisations gain confidence in their suppliers and increase visibility into their supply chains.

Cyber Essentials as a supply chain tool

With the financial services sector facing an evolving cyber threat, St James's Place, one of the UK's largest pensions & life companies, asked its partnership network of over 2,800 independent businesses to certify to Cyber Essentials Plus.

In such a large supply chain, this had its challenges, but the decision is already showing a positive impact.

> "Security incident numbers have significantly reduced... we have seen around 80% reduction in cyber security incidents, which directly correlates to controls and best practice implemented through Cyber Essentials."
>
> **Matthew Smith, Divisional Director of Cyber Security, St James's Place.**

Cyber Essentials future ambitions

Technology is driving better connection, productivity and opportunity for UK organisations, but with greater cyber capabilities comes additional complexity and risk. More than ever, it is critical for organisations to have fundamental cyber security controls in place and to be protected from cyber attacks. We know the Cyber Essentials scheme is helping organisations, large and small, do just this. Certified organisations are more secure, more protected and better placed to embrace the full benefits of digital growth.

Uptake of the scheme continues to grow with 23% year-on-year growth for Cyber Essentials and 28% for Cyber Essentials Plus. This is great progress, however, we need the rate of growth to increase. To improve UK cyber resilience we need many more organisations across the UK to be Cyber Essentials certified, or working towards certification. To this end, the Department for Science, Innovation and Technology (DSIT) is working closely with the National Cyber Security Centre (NCSC) and industry to stimulate market-driven demand for the scheme, by promoting the role Cyber Essentials can play as a tool to assure cyber security in the supply chain.

Cyber risk within supply chains is increasingly prevalent. Just 11% of UK organisations assess cyber risk in their immediate suppliers, so it is clear organisations must do more to mitigate this risk. The DCMS Supply Chain Call for Views found that organisations consider a lack of assurance tools, insufficient expertise and a lack of visibility as significant barriers to managing supplier cyber risk. This presents a dangerous scenario where supply chain attacks are increasing, while minimal efforts are being made to address this increased risk. Requiring suppliers to have Cyber Essentials increases cyber security across supply chains, while providing a tangible way for organisations to gain confidence in the cyber security of their suppliers, particularly where the above barriers are present.
As such, the role Cyber Essentials plays as a third-party assurance tool is integral to our future ambitions for the scheme.

As we work to increase demand for Cyber Essentials, we also have to ensure all organisations are able to get certified and are supported during the process. That is precisely why the NCSC has developed the *Pathways* and *Cyber Advisor* initiatives within Cyber Essentials. Through *Pathways*, we are exploring how to provide large, complex organisations which struggle to meet the strict Cyber Essentials controls with an alternative route to certification. Through *Cyber Advisor,* we are ensuring NCSC assured support is available to small and medium-sized organisations which are working toward Cyber Essentials certification. These programmes are integral to the future success of the scheme.

We want all businesses and charities which rely on technology to be aware of the scheme, to want to be certified and to be supported in the process. As the number of organisations with Cyber Essentials increases, so too will the cyber resilience of the UK, contributing to the government's work to improve UK cyber defences and protect our economy and essential public services.

Department for Science, Innovation & Technology

Cyber Essentials is recommended as the minimum standard of cyber security that every organisation – no matter its size - should aim for.

Get certified, find support or discover more about Cyber Essentials; visit the NCSC's Delivery Partner, IASME: iasme.co.uk/cyber-essentials.

iasme

Did you know... The Customer Service Team at IASME answer an average of 2400 email queries a month about Cyber Essentials.

NCSC

ncsc.gov.uk/cyberessentials

national-cyber-security-centre

cyberessentials@ncsc.gov.uk

National Cyber Security Centre

Department for Science, Innovation & Technology