The Final Step.
Professional IT

Your Guide to Cyber Essentials.

Take steps to protect your business from cyber attacks

What is Cyber Essentials?

Cyber Essentials is a framework of fundamental cyber security protections organisations can be assessed against. These essentials help keep you and others safe from cyber crime.

It was developed by the Government in partnership with the National Cyber Security Council (NCSC) and highlights five basic security control measures you should have in place.

There are two levels of certification, delivered by the Information Assurance for Small and Medium Enterprises Consortium (IASME):

Cyber Essentials

A self-assessment form with questions based on the five controls, verified by an online assessor against the standard.

Cyber Essentials Plus

The same process, but in addition, you submit to a technical audit that verifies your measures work.

An organisation certified in Cyber Essentials is demonstrating to their shareholders, staff and clients that they take security seriously and have invested money and time in improving it.

Cyber security is complex. This framework makes it easier to rise to the challenge of meeting your responsibilities.

Why is Cyber Essentials so important to businesses ?

We all know at the core of any business relationship is trust.

As cyber crime grows, no business can afford to work with organisations they cannot trust with security. Data is precious. Any organisation, no matter their size, industry and technical know-how, can have it stolen and compromised by criminals.

Cyber Essentials is concrete evidence that you have turned your good intentions around cyber security into action, which is something that more and more clients are assessing when looking at organisations. The IASME website makes it easy to see who is certified in Cyber Essentials and if you meet the standard.

What CEOs should understand about Cyber Essentials.

Cyber Essentials is not an invincibility shield... but it is a great place to start!

As the name suggests, Cyber Essentials only covers the basic security protocols that every organisation should have in place.

The current standard aims to protect you from **80%** of risks

But it cannot guarantee safety and you shouldn't ignore the other **20%**

IASME CONSORTIUM

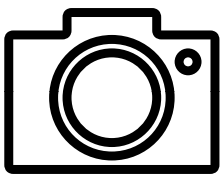
"Cyber Essentials represents the Government's minimum baseline standard for Cyber Security in the UK"

It only takes one cyber security incident for your organisation to experience severe financial and reputational damage.

In addition to this, cyber criminals are renowned for targeting organisations that appear complacent and unprotected, like small businesses that assume due to their size they will never be targeted. If you have this mindset, criminals see you as low-hanging fruit.

Easy to breach, easy to extort.

Cyber Essentials is a snapshot in time of your IT



It indicates if your organisation at that time met the standard. Even organisations with the best security posture possible, will find it erodes over time and requires annual appraisal and updates.

But the more time, money and effort you invest in security, the less likely you are to face a breach, and suffer long-lasting consequences.

With its additional technical audit, many organisations invest in Cyber Essentials Plus

Many businesses when doing due diligence specifically seek it out at as a sign of good cyber security. This is because Cyber Essentials Plus has a higher level of verification, making it a more "trusted" standard.

Being able to talk about the importance of Cyber Essentials and its limitations helps build trust with partners.

What value can your business get from Cyber Essentials?

It saves you money

The most immediate value is that is saves you money.

Cybercrime cost the UK **£3.1 billion**[1] in 2021

and is predicted to cost heights of **£1 trillion**[1] in 2022

Average ransomware payment has risen by **↑71%**[3]

As well as the costs of criminal extortion, cyber crime costs in terms of: lost productivity, lost business, paying for external recovery experts, legislative fines and additional insurance.

Average cost of a data breach for small to medium businesses in the UK is **£6,490**[2]

Average ransom paid in 2022 **£925,162**[3]

Secure new business

Good cyber security also helps secure new business and reassure existing customers. Companies do due diligence when considering a supplier to evaluate who is suitable.

Certifications are being used now to assess if companies meet an acceptable security benchmark, and if they don't they are crossed off.

Once you gain your Cyber Essentials certification you will be listed on IASME's directory of organisations awarded Cyber Essentials.

Protect your reputation

In addition to financial costs, being the victim of a cyber attack incurs significant reputational damage.

Studies are showing that more and more people in the UK are choosing who to do business with based on their cyber security.[4]

Often organisations stop working with those who put their data at risk and can't offer compelling evidence of having taken their responsibilities seriously.

1. www.comparitech.com/blog/information-security/uk-cyber-security-statistics
2. www.dbxuk.com/statistics/data-breach-statistics
3. www.dbxuk.com/statistics/data-breach-statistics
4. www.thefinalstep.co.uk/bytesizebulletins/uk-consumers-would-pay-for-control-of-their-data

The business benefits of Cyber Essentials.

Fulfil your responsibilities

It also helps you fulfil your legal and moral responsibilities to keep data safe.

The Government wants the UK to be a safe place to do business, so it wants business leaders to take action. Cyber Essentials helps you frame how you can do this.

ico.

The Information Commissioner's Office (ICO) recommends Cyber Essentials.

GDPR.EU

Cyber Essentials helps with UK GDPR regulations, ISO and other standards.

National Cyber Security Centre

It ties in with the National Cyber Security Council's (NCSC) Ten Steps to Cyber Security.

It is critical business owners understand and are actively involved in their own security. Increasingly, C-level executives are getting held to account by clients and the ICO who are expecting better organisational risk assessment and mitigation.

Safeguard your business

By investing in Cyber Essentials you will reduce your risk of being targeted by cyber criminals.

With so many organisations investing in Cyber Essentials, criminals specifically seek organisations out that have visibly paid less attention to their security (they can even check online to see which companies have and have not taken this preventative step).

We all recognise how leaving our doors or windows open when we leave the house is not smart or responsible.

But often we excuse ourselves from making the same errors around cyber security. It's too abstract, or too technical or too much of a headache.

You can't pass responsibility to the IT department and/or insurance and forget about it.

Cyber Essentials helps you take charge and develop the security first mindset that will allow you to mitigate and respond to risks effectively and quickly.

FREE cyber liability insurance

Cyber Essentials certification includes insurance for UK-domiciled organisations with a turnover under £20m.

Of course this may conflict with separate, more comprehensive cyber insurance you have arranged, so you may want to refuse or cancel this insurance.

Changes to Cyber Essentials.

Like cyber crime, Cyber Essentials is continually evolving

Cyber Essentials is constantly expanding its method and scope of assessment and recommended best practices. This is because cyber security is a rapidly evolving field, with criminals developing increasingly innovative and sophisticated methods to extort and infiltrate organisations every day.

Maintaining your accreditation shows you are taking account of and adjusting to the latest risks.

Working from home, cloud services and mobile devices are more and more popular. But they introduce greater complexity and risks that the Cyber Essentials standard is evolving to address.

These new standards may mean putting new security measures in place. We recommend planning ahead and seeking expert advice in order to ensure you maintain your accreditation.

Easy 4-step certification process

1. Cyber Essentials Audit

We start with a Cyber Essentials Audit. This will help you understand the current state of your IT as compared to the Cyber Essentials standard.

2. Gap analysis

We produce a list of the gaps you need to close to certify.

3. Remedial action plan

This is a key phase to ensure the best chance of certifying.

It's a discussion of how best to close any gaps and who is best placed to certify them. It's coordination between us, any in-house IT you have and the external assessor.

4. Submit assessment and verification

- A form is submitted to IASME and is verified online to gain Cyber Essentials.
- If you are certifying to the Plus level you then have three months to do a technical audit and certify to the higher level.
- Certification confirmed and issued. A reminder is set to renew the following year. This process normally starts about three months before the expiry date.

The 5 key protections of Cyber Essentials.

Secure Configuration

Secure configuration and network management. Servers, network devices and computers are set up to keep them functional but minimise any vulnerabilities.

Access Control

Hackers want to get administrator access so they can do what they want. It's important to verify who has access to what level, even at the sacrifice of some convenience.

Malware Protection

There's a large range of malware and delivery mechanisms. Keeping it out and detecting it when it does get in are key components of protecting against threats such as ransomware.

Firewalls and Routers

With boundary firewalls and internet gateways you have a private network with "rules" set to protect who can get in and where they can access.

Security Updates

Software and systems have inherent vulnerabilities. As they are discovered and fixed (called patching), you need to apply that patch as quickly as possible.

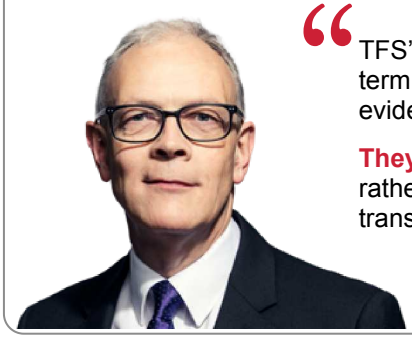
"The Final Step provides a professional, user-friendly, solutions-focused service.

I have recommended them to many contacts.

Valued client for 25 years

Laura Devine
Managing Partner
City of London, London

LAURA DEVINE IMMIGRATION



Valued client for 5 years

"TFS's philosophy of building long-term working relationships is evident throughout.

They care about partnership rather than just short-term transactions.

Peter Martin
Director
Westminster, London

inter musica

SmileBack
100/100

Based on 401 reviews in the last 90 days

Google Reviews ★★★★★

4.6 Stars, based on 25+ Reviews

Channel Futures MSP 501 2022 WINNER

Gold Microsoft Partner

Microsoft

CYBER ESSENTIALS CERTIFIED PLUS

020 7572 0000 contact@thefinalstep.co.uk www.thefinalstep.co.uk