# The Ultimate Guide to Cyber Essentials

Every question you've ever had about Cyber Essentials answered.

**Cyber safe.**

**Cyber assured.**

CYBER ESSENTIALS

## KEY BENEFITS

p.8-9

- Prove to clients and stakeholders that you're secure
- Save on insurance premiums
- Gain an edge over competitors
- Win new business tenders
- Avoid 80% cyber threat

## THE CYBER ESSENTIALS PROCESS

p.15

1. Speak to Us
2. Achieve Cyber Essentials (Basic) certification
3. Pre-Assessment
4. Achieve Cyber Essentials Plus certification

## 5 CRITICAL CONTROLS

p.11-14

- Secure Configuration
- Patching
- Access Control
- Malware Protection
- Firewalls and Internet Gateways

## IASME AND THE CYBER ESSENTIALS SCHEME

p.10

IASME CONSORTIUM

- Cyber Essentials Scheme p.5
  - Cyber Essentials Basic p.6
  - Cyber Essentials Plus p.6
- IASME Governance

## PDSC CERTIFICATION

p.16

PDSC POLICE DIGITAL SECURITY CENTRE

Support your cyber efforts by achieving the Police 'Digitally Aware' Badge in under 20 mins!

## POST CERTIFICATION

p.17-18

Daily Compliance to Cyber Essentials Plus

Maximum Risk Reduction with SOC & SIEM

CYBER ESSENTIALS

Cyber Essentials seems to be everywhere, but what does it truly mean for your organisation? We've created the Ultimate Guide to Cyber Essentials to help you understand the fundamentals as well as the technical aspects of Cyber Essentials without the complicated jargon.

Every single question you have around Cyber Essentials will be answered and that's a promise! So, take a seat, grab a cuppa and put your feet up while we explain everything you need to know about Cyber Essentials.

# Contents

# Understanding the threat to your organisation

Can we be honest with each other for a second? On a scale of 1-10, how much do you really understand the world of cybersecurity?

Despite the fact most organisations spend 5.6% of their overall IT budget on security and risk management, many organisations still don't understand what cybersecurity is and subsequently, they don't know how to keep hackers out.

Over the last 10 years, we've seen a massive growth in cybercrime. According to data from the UK Government's Cyber Breaches Report in 2020, 46% of UK businesses reported cyber breaches in the last 12 months - and those are just the cases that were reported! Unfortunately, these numbers are only rising as we become more and more reliant on technology within our organisations.

UK businesses are experiencing an estimated 65,000 cyber attack attempts daily. The message is clear: Cyber security needs to be a priority for every business owner.

As you can imagine, there's a significant number of organisations wishing they could go back and make amends. The popular phrase "It's never too late" clearly does not apply to cybersecurity.

CYBER ESSENTIALS

# Who is a threat to your organisation?

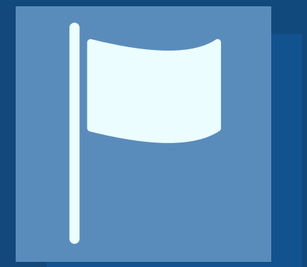
Whether it's an accidental error by one of your employees or a hacker half-way around the world attempting to gain access to unauthorised data, there are five common sources of the cyber threat which are shown below:

**Hacktivists**
Agenda or ideology.
Examples are: Anonymous, Syrian Electronic Army.

**Insiders**
Privileged access to data.
Can be malicious or, more commonly, accidental.

**Hackers**
Status and technical challenge. Can be good or bad depending on their actions.

**Criminals**
Often driven by financial gain. Theft of data ransomware cyber-enabled or dependant.



**State Sponsored**
National advantage.
Well-funded and targeted.
Gather information.

CYBER ESSENTIALS

## What are cybercriminals trying to do to your organisation?

Cybercriminals have many different ways to get your data, for instance:

- Infect your systems with malware (ransomware) - malware is software that is specifically designed to disrupt, damage, and gain unauthorised access to your computer systems.
- Use Social Engineering - the use of deception to manipulate your employees into divulging confidential and personal information that will be used for fraudulent purposes.
- Exploit vulnerabilities - weaknesses in your systems that can be exploited by an attacker. Vulnerabilities exist within all systems and software. The challenge is ensuring that your systems are constantly up to date and that vulnerabilities are identified and remediated quickly to ensure your risks are mitigated and your attack surface reduced.
- Overload with DDoS (Denial of Service) - hackers use multiple systems to flood and target the bandwidth and resources of your systems. Your website and systems receive so many requests that they are unable to deliver a response and either fail completely or just stop responding to any legitimate requests.

CYBER ESSENTIALS

### How do they do this?

The attackers use a control server and issue a command to ask all the compromised systems in control of the server to send requests to your website or system all at the same time.

# What is the solution to the cyber threat?

During 2020, 46% of UK organisations suffered a data breach or attack. We know that sounds terrible, however, the good news is that businesses are starting to prioritise their cybersecurity, with now 80% saying it is a high priority for their senior management boards.

So how are these businesses responding to the cyber threat?

Well, a lot of people have been talking about Cyber Essentials recently and rightly so. With the ever-growing push from the government, clients and suppliers, you've probably already heard of it too. So why is everyone talking about Cyber Essentials? Quite frankly, because it works.

UK organisations are beginning to prioritise cybersecurity by implementing Cyber Essentials.

# What is Cyber Essentials?

Cyber Essentials is a UK government information/data assurance scheme operated by the National Cyber Security Centre (part of GCHQ) that encourages organisations to adopt good practices surrounding data security. Cyber Essentials has been designed by the government to make it easy for you to protect your organisation against common cyber threats.

Think of it like this, you're in the middle of your driving test, hoping to achieve your driving licence. The assessor in the passenger seat understands what you need to do in order to pass and the assessor will be using a checklist to determine whether you pass or fail.

The company certifying your organisation are the assessor (called a Certifying Body) and Cyber Essentials is the checklist. Cyber Essentials is the standard to compare the current condition of your cybersecurity against. The aim is to reach the Cyber Essentials standard and once this is done, you achieve the Cyber Essentials certification and your organisation will have reduced its cyber threat immensely.

Not too complicated right?

The reason the government's 'Department for Business, Innovation and Skills' created Cyber Essentials in 2014 was to ensure all suppliers doing business with the UK government are responsibly handling any personal and sensitive data they possess.

It's important to remember Cyber Essentials gives you a "point in time snapshot" assessment of your organisation and the certification is annual, which means you'd need ongoing security solutions such as SOC & SIEM on top of your Cyber Essentials certification to be able to have complete peace of mind to understand your cybersecurity on a daily basis.

CYBER ESSENTIALS

# How many certifications are there for Cyber Essentials?

There are two certifications for Cyber Essentials - Cyber Essentials and Cyber Essentials Plus. They are both achieved in different ways and both respectively have their own benefits for your organisation.

To understand which certification you need for your organisation, it is important to understand the difference between the two certifications.

# Achieving Cyber Essentials

Cyber Essentials 'Basic' is a 'DIY' certification. It can be completed by your organisation's own IT department or a certified, external third party if you don't have the capacity or technical expertise in-house. Your organisation completes a self-assessment questionnaire and the responses are then independently reviewed by an external certifying body.

CYBER ESSENTIALS

# Achieving Cyber Essentials Plus

Cyber Essentials Plus requires an external certifying body to carry out the system tests rather than the 'DIY' nature of Cyber Essentials.

# Cyber Essentials vs Cyber Essentials Plus

A Cyber Essentials certification shows your clients and customers that you care about your cybersecurity whereas Cyber Essentials Plus shows you are doing absolutely everything in your control to protect their data and this is verified by an 'auditor'.

Cyber Essentials Plus requires the use of an external certifying body throughout the entire certification process, whereas Cyber Essentials uses an external certifying body to examine the responses from the self-assessment questionnaire.

# Why do you need a Cyber Essentials Plus Pre-Assessment?

We always recommend completing a Pre-Assessment before purchasing Cyber Essentials Plus. There are many reasons why you need the Cyber Essentials Pre-Assessment but the main purpose of it is to highlight which areas of your cybersecurity require attention and improvement.

The last thing you want to be doing is wasting money and the Pre-Assessment makes sure that you won't do that. When you do the Pre-Assessment with us, one of our Senior Cyber experts will guide you through the complete report to ensure you make the correct remedial actions in order to pass the actual assessment, so you can avoid any re-certification costs!

We'll basically tell you where you are with your security and show you what is required to address the issues identified. With these issues identified and fixed, you will be in a much better place to secure the Cyber Essentials Plus certification.

It's a no brainer!

# What are the benefits of Cyber Essentials?

- Cyber Essentials is the only government-backed UK cybersecurity standard, which means you will be aligning yourself with the most recognised standard in the country.

- Time. Money. Resources. With a bird's eye view of your cybersecurity from the executive level, you can iron out any inefficiencies in your practices as well as maximising productivity as your team will have more time on their side.

- You've always dreamt of landing that HUGE government contract, without Cyber Essentials, you'll have to stop dreaming. Being Cyber Essentials certified is a minimum requirement for any organisation looking to obtain government contracts (including the Ministry of Defence), and increasingly so in the private sector.

- Whilst the Cyber Essentials certification shows that you care about data, the Cyber Essentials Plus certification shows that you're making every effort to protect data.

  This will make a big difference when your organisation is trying to obtain cyber insurance - as the brokers will be willing to offer you a reduced premium, as they can see your organisation is incredibly cyber safe.

- We're sure you utilise services, you are a client to someone. Now think of the reassurance you'd feel if that service came back to you and said "we're doing absolutely everything in our power to protect your data and can prove it because we have the governments own standard". You'd appreciate the work they do even more than you do currently.

  This is the same feeling you want to give to your clients. You want your clients to appreciate what you do for them. It begins with protecting your clients and before you know it, you've enhanced your reputation in your industry. The industry will recognise you as one of the safest organisations in the sector, you can only begin to imagine what that could do for your organisation.

CYBER ESSENTIALS

# What are the benefits of Cyber Essentials?

There are organisations that simply do not care about cybersecurity, they believe it is not a priority and that they will never have a problem with it. It's an unfortunate way of thinking, their organisations won't last long in this day and age. Ideally, you'd want to separate your brand and identity from these organisations.

With a Cyber Essentials certification, you automatically show that you care about data as well as differentiating yourself from your competitors who have yet to prioritise their cybersecurity. Think of it now, your website will be updated with the Cyber Essentials logos and you will have put your organisation amongst an elite group of organisations in your industry who have shown they care about their data. If you show your clients you care about them, they'll care for you too.

The UK is still required to comply with GDPR (General Data Protection Regulation). It's important to comply for many reasons, but here's one that particularly stands out - your organisation could be liable to pay up to 4% of your turnover if breached.

The reason for this is the Information Commissioner's Office (ICO) can very quickly conclude that you did not do everything in your power to protect the data you hold. How? They can see you didn't have Cyber Essentials when you were breached. Simply having the certification could have prevented the fine as they could see you did try to protect your data.

Can your suppliers trust you? If something went wrong, what are the chances they'd continue to do business with you?

Statistically, most suppliers end relationships with clients who suffer a breach. If you're wondering why, it's because they find out you did little to protect their data in the first place and this means the trust you had built has been lost. Without trust, the supplier does not want to do business with you any longer.

With a Cyber Essentials certification, you will be protecting your organisation and therefore, you're giving your suppliers the trust they need to continue working with you. The choice is clear, you can give your suppliers uncertainty without Cyber Essentials or you can give them certainty with Cyber Essentials.

CYBER ESSENTIALS

# Introducing IASME – The Cyber Essentials NCSC Partner

The IASME Governance Standard

The Cyber Essentials Scheme

On 1st April 2020, it was announced that The IASME Consortium would become the sole accreditation body for Cyber Essentials in the United Kingdom. Prior to this, there were five accrediting bodies with varying methodologies, however, it was decided by the Government that it would be more beneficial if all Certification Bodies operated under the same methodology.

In addition to the NCSC's Cyber Essentials scheme, IASME also offers the IASME Governance standard, which is designed specifically for SMEs (small and medium-sized organisations) and offers a similar level of assurance to the internationally recognised ISO 27001 standard, but is simpler and often cheaper for SMEs to implement. The IASME Governance Standard is risk-based and includes aspects such as physical security, staff awareness and data backup.

# Getting started with Cyber Essentials

The reason Cyber Essentials can protect your organisation from 80% of the cyber attacks is by ensuring that you are aligned with the five critical controls. You're probably thinking... what on earth is a control? Simply, technical controls are safeguards that are incorporated into computer hardware, software, or firmware. The controls for Cyber Essentials are:

**Access Control**
You are able to control which members of your team can see certain data.

**Firewalls and Internet Gateways**
Cyber Essentials requires all devices that are connected to the internet to be protected with a firewall.

**Secure Configuration**
Your settings will be more secure making it harder for hackers to break into your systems.

**Patch Management**
It is crucial to have your devices updated to ensure vulnerabilities can be found and solved.

**Malware Protection**
Cyber essentials will help protect your data from viruses, malware and other threats to your business.

CYBER ESSENTIALS

# Access Control

It is important to only give users access to the resources and data necessary for their roles, and no more. All users need to have unique accounts and should not be carrying out day-to-day tasks, such as invoicing or dealing with e-mail whilst logged on as a user with administrator privileges, which allow significant changes to the way your computer systems work.

### Best Practices

- You should ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in your organisation.
- You should ensure that no devices can be accessed without entering a username and password. Users should not be able to share accounts.
- Stop any former employee accessing any of your systems.
- Ensure that staff only have the privileges they need to do their current job.
- You should have a formal, written-down process that you follow when deciding to give someone access to systems at administrator level. This process should include approval by a person who is an owner/director/trustee/partner of the organisation.
- You should ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware.
- You should ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.
- You should track by means of a list or formal record all people that have been granted administrator accounts.
- You should review the list of people with administrator access regularly. Depending on your organisation, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.
- Enable two-factor authentication for all administrative accounts.

CYBER ESSENTIALS

# Firewalls and Internet Gateways

Firewalls are the technical protection between your systems and external systems. It is the firewall that will filter anything that could be of harm to your systems.

Internet Gateways enable us to communicate by sending data back and forth. Without gateways, the Internet wouldn't be of any use to us.

### Best Practices

- Your home-based workers should be using a firewall or an office VPN.
- Your router or hardware firewall device will have default passwords which should be changed to passwords that are hard to guess and at least eight characters in length.
- You should have a guest network for your clients and customers for when they want to use your servers. For instance, if a customer wants access to your WiFi, you should offer them the guest option as otherwise, you will be making your network susceptible to an attack.

- If you allow other people such as your managed service provider to access your settings via the internet, you should have two-factor authentication set-up or add them to the trusted list of IP addresses.
- You should enable firewalls on all your connected devices.

## Secure Configuration

It's rare for computers to be secure straight out of the box as they often include an administrative account with a publicly known default password, unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed non-essential applications or services. All of these can present security risks.

### Best Practices

- You should look to remove or disable the applications, system utilities and network services that are not needed in day-to-day use.
- Remove or disable any user accounts that are no needed in day-to-day use on all devices.
- Change the default password for all user and administrator accounts on all devices and servers to a non-guessable, strong eight or more character password.
- Ensure each user and administrator has a non-guessable, strong eight or more character password.
- You shouldn't include predictable words such as "password" or predictable sequences such as "12345".

CYBER ESSENTIALS

- Prevent people outside of your organisation from accessing confidential information through your external services (VPN server, mail server etc) by making this information private.
- Change passwords as soon as you believe they have been compromised.
- Limit the number of unsuccessful login attempts to no more than ten within five minutes.
- Create a password policy to guide your users. This includes guidance on how to choose non-guessable passwords, not to use the same password for multiple accounts, which passwords may be written down and where they can be stored.
- Disable auto-run and auto-play on all of your systems.

## Patch Management

To protect your organisation, you should ensure that your software is always up-to-date with the latest patches. This is a requirement of Cyber Essentials.

### Best Practices

- Ensure all operating systems, applications and firmware on your devices are supported by a supplier that produces regular fixes for any security problems.
- Use licensed software in accordance with the publisher's recommendations.
- Ensure all high-risk or critical security updates for operating systems and firmware are installed within 14 days of release.
- Remove older applications from your devices that are no longer supported by the manufacturer.

# Malware Protection

Malware (known as ransomware) is generally used to steal or damage information. Malware is often used in conjunction with other kinds of attack such as ‘phishing’ (obtaining information by confidence trickery) and social network sites (which can be mined for information useful to a hacker) to provide a focussed attack on an organisation.

## Best Practices

- Install anti-malware software.
- Have a list of approved applications and only use and install these applications.
- Update anti-malware software daily.
- Scan files automatically upon access to anti-malware software.
- Your anti-malware software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites.
- Restrict users from installing unsigned applications.
- You should create a list of approved applications and ensure users only install these applications on their devices including employee-owned devices.
- If using application sandboxing, ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and your local network.

CYBER ESSENTIALS

# The Cyber Essentials Process

**Step 1: Speak to Us**
Let us know more about your business so we can assess your current situation and offer guidance on whether your business needs Cyber Essentials or Cyber Essentials Plus.

**Step 2: Achieve Cyber Essentials (Basic) certification**
We will guide you through the process of getting your business certified for Cyber Essentials. This usually takes less than 24 hours. You'll get your logos, certificate and report straight after achieving certification.

**Step 3: Pre-Assessment**
With over 95% of businesses failing Cyber Essentials Plus in their first attempt, we will ensure you pass Cyber Essentials Plus first time, by highlighting any existing issues and so your IT provider can fix them before the actual Cyber Essentials Plus assessment.

**Step 4: Achieve Cyber Essentials Plus certification**
We have the ability to certify for Cyber Essentials Plus remotely. After assessment and all issues remediated, you will have passed Cyber Essentials Plus and you'll get your logos, certificate and report straight after achieving certification.

CYBER ESSENTIALS

All our assessments are done 100% remotely. This means we can assess your homeworkers, so you don’t have to go to the office to meet anyone or plug in a scanning device/pc. The price is for the whole network and covers ALL your physical sites and ALL your employees - wherever they are in the world.


# The Police 'Digitally Aware' Certification

In early 2021, we began working with The Police Digital Security Centre, meaning we are now able to offer their 'Digitally Aware' cyber certification.

While not an alternative to Cyber Essentials, it can be a great stepping stone for SMEs just starting out on their Cybersecurity journey or can be taken in conjunction with Cyber Essentials for an extra badge of honour that will show your clients that you are cyber aware and taking steps to ensure your business is cyber secure.

The assessment itself only takes 20 minutes through an easily accessible online portal, and you'll be able to download the Police badge to put on your website and collateral immediately after a successful pass.

It's an add-on not to be missed!

PDSC
POLICE DIGITAL SECURITY CENTRE

CYBER ESSENTIALS

# Post Certification

Once you have achieved Cyber Essentials/Plus, you will be able to display appropriate Cyber Essentials logos on your website and will have reduced your cyber threat by 80%. However, this still leaves a 20% gap, so how do you tackle that?

**Step 5: Daily Compliance to Cyber Essentials Plus**
Ongoing Compliance to ensure your business is constantly aligned with the Cyber Essentials Plus standard.

## What is Compliance?

The difficulty with Cyber Essentials certifications is that they're only 'point-in-time' assessments, renewed every 12 months. A vulnerability could emerge during that period without you might not realise before it's too late. Wouldn't it be great if you knew every single day whether your business was still aligned with the Cyber Essentials Plus standard?

Our Compliance solution does this by running daily audits on all your systems checking for vulnerabilities and signs that you're no longer compliant with Cyber Essentials Plus.

Your own cyber dashboard gives you regular status updates so you know immediately if something requires attention from your IT provider.

This ongoing Compliance solution is a simple installable agent which can easily be switched off or upgraded to the higher-level SOC & SIEM service...

CYBER ESSENTIALS

# Post Certification

**Step 6: Maximum Risk Reduction with SOC & SIEM**

You can reduce your risk of breach by 98% by implementing proactive SOC and SIEM solutions that monitor and reacts to cyber threats.

## What is SOC & SIEM?

A SIEM (Security Information and Event Management), is a tool that indicates suspicious activity through set-up rules and correlation intelligence and enables security analysts to act on suspected threats.

A SOC (Security Operations Centre) encompasses the people, processes, as well as technology involved in protectively-monitoring a network, responding to incidents, and researching/actively searching for known/unknown threats.

### What does this mean for your organisation?

A SOC works best with a SIEM, as the SIEM provides the foundation for the SOC's specialised security analysts to work on the threats presented by the SIEM. Whilst a SIEM is the best tool for collecting and correlating information from your organisation, what happens when you get an alert? You need a set of skilled security analysts to help you understand what those alerts mean and that's where SOC comes in.

By having SOC & SIEM for your organisation, you will be able to proactively monitor threats posed to your organisation and be able to prevent breaches and attacks before they happen. As Cyber Essentials shows you a "snapshot" of your cybersecurity at a specific time, the SOC & SIEM will ensure you are always up to the standard. This is hugely important as you could save money the following year when renewing Cyber Essentials as you may not need a pre-assessment.

Microsoft 365

We can offer two flavours of SOC & SIEM. You can get full-blown endpoint protection or a more specific SOC & SIEM solution that centres around Office 365 Services. With more and more businesses using Microsoft's applications, this is a great option for protecting your most important assets against cyber threats.

CYBER ESSENTIALS

CYBER ESSENTIALS

# Additional FAQs

**Does Cyber Essentials expire?**

Cyber Essentials will require annual renewal and the amount you pay depends on your certification.

**Why should I renew my Cyber Essentials?**

For the same reasons you chose to certify in the first place:

- To reduce your cyber threat by 80%
- To benefit from the Cyber Essentials scheme
- To understand your organisation's cybersecurity position

**Can I achieve Cyber Essentials Plus without Cyber Essentials Basic?**

To be able to achieve Cyber Essentials Plus, you must first achieve Cyber Essentials Basic.

**How do I become 100% secure?**

We'd all love to be 100% secure, unfortunately, this is all but impossible. The best thing you can do is guarantee 80% protection from cyber-attacks through Cyber Essentials, and then look to invest in Compliance and SOC & SIEM solutions to bridge that gap. Then consider getting specialist cyber insurance so you can be protected should experience a cyber attack.

**I've been told to buy tools, why should I bother with Cyber Essentials?**

Tools are good, but they're not cheap. It is much better to see cybersecurity tools as a supplement to Cyber Essentials certifications. With Cyber Essentials, you'll automatically reduce your cyber threat by 80% and then you can bring in additional tools to bridge the gap from 80% to 100%. Get certification sorted first, then invest in further tools.

**How quickly can I become certified for Cyber Essentials and Cyber Essentials Plus?**

You can become certified within 24 hours for Cyber Essentials and then to upgrade to Cyber Essentials Plus, you'll need to achieve the certification within 3 months of achieving Cyber Essentials.

**It’s your duty to protect your stakeholders.**

The cyber threat is real and it’s coming for every single organisation. With almost half of British organisations suffering an attack in 2020, it’s up to those organisations to do their best to protect their stakeholders with essential and fundamental investments - such as Cyber Essentials. With Cyber Essentials, your organisation can have peace of mind that it's protection against 80% of cyber attacks, reassure your customers and avoid huge fines from the ICO post-breach.

# Get Certified Today

CYBER ESSENTIALS