SW-IT
INSPIRATION.TECHNOLOGY
www.sw-it.co.uk | 01305 500118

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

The Ultimate Guide to Cyber Essentials

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

Cyber safe.

Cyber assured.

IASME CONSORTIUM

CERTIFICATION BODY 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 both the fundamentals and the technical aspects of Cyber Essentials without the complicated jargon.

So, take a seat, grab a cuppa and put your feet up while we explain everything you need to know.

Contents

Understanding the threat to your organisation

Let's be truly honest for a moment. On a scale of 1-10, how much do you really understand the world of cyber security?

Despite the fact most organisations spend 5.6% of their overall IT budget on security and risk management, many still don’t understand what cyber security 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, 39% of UK businesses reported cyber breaches in the previous 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 and hackers get more sophisticated.

UK businesses are experiencing an estimated 65,000 cyber attack attempts daily.

The message is clear: cyber security must be a priority for every business owner.

As you can imagine, there is a significant number of organisations wishing they could go back and make amends. The phrase “It’s never too late” sadly does not apply to cyber security.

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 unauthorised access to your data, there are five common sources of 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. Desgined to 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. Often this is done using a control server where a command will be issued to ask all the compromised systems in control of the server to send requests to your website or system all at the same time. 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

What is the solution to the cyber threat?

During 2020, 39% of UK organisations suffered a data breach or attack. We know that sounds uncomfortably high, however, the good news is that businesses are starting to prioritise their cyber security, with 77% now saying it is a high priority for their senior management boards.

So how are these businesses responding to this cyber threat?

Well, a lot of companies are looking to recognised standards that will give them a baseline for good cyber security. One of the UK's most recognised standards is Cyber Essentials and with the ever-growing push from the government, clients and suppliers, you've likely heard that name knocking around too.

So why is everyone talking about Cyber Essentials? Quite frankly, because it works.

UK organisations are seeing the benefit of aligning their security to the requirements of Cyber Essentials and it is these efforts that are largely responsible for the decline in successful breaches over the years.

What is Cyber Essentials?

Let's dig into what the scheme involves and why it's relevant to you - after all that's probably why you downloaded 'The Ultimate Guide to 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 was designed by the government in 2014 primarily for small to medium-sized businesses to make it easier for them to protect against common cyber threats.

You can think of it as a bit like a driving test. There are certain requirements you have to fulfil in order to pass successfully, and your assessor will confirm whether you meet these.

For Cyber Essentials, that 'assessor' is what's called a Certification Body, and they have the official qualification needed in order to certify you for Cyber Essentials - that is as long as your organisation ticks all the boxes. A large portion of the assessment is a questionnaire and it is these answers that will determine whether you pass or fail.

Once you can show you have all the necessary processes, policies and controls (more on this later) in place, you'll be awarded a certification which you can show off to all your clients, partners and suppliers and most importantly, you'll feel more confident that you're secure and protected.

Not too complicated right?

The certification must then be renewed on an annual basis to account for any changes both to your own company's infrastructure and to the wider security landscape over the course of 12 months.

CYBER ESSENTIALS

Certification Bodies and IASME

The IASME Governance Standard

The Cyber Essentials Scheme

As mentioned, Certification Bodies are an essential part of achieving your Cyber Essentials certificate. But what exactly are they and how do you find one? Certification Bodies operate under the IASME Consortium who, as of 1st April 2020, are the sole accreditation body for Cyber Essentials in the United Kingdom. Prior to this, there were five accrediting bodies with varying methodologies, but it was decided by the Government that it would be more beneficial if all Certification Bodies operated under the same methodology.

IASME now works with several Certification Bodies across the country and each Certification Body has qualified assessors who have the ability to certify businesses and organisations for Cyber Essentials.

It's also worth noting that 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 it 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.

Achieving Cyber Essentials

Now you understand how the scheme is delivered and who actually certifies your organisation, let's look at what's actually involved in the process of achieving Cyber Essentials.

Technically, there are actually two assessments you need to complete in order to be fully certified for Cyber Essentials. The 'Basic' certification must be achieved first (you must submit the assessment within 6 months of receiving it), and this is then followed by the more comprehensive 'Plus' assessment. The processes for both are slightly different but you'll soon learn how both work together and benefit your organisation.

Cyber Essentials ‘Basic’ is a kind of DIY certification that comes in the form of a self-assessment questionnaire (SAQ). It is usually completed by an organisation’s own IT team or external IT provider, but must then be independently reviewed by an official Certification Body. Many Certification Bodies actually offer expert guidance, which is strongly advised if you want a stress-free pass!

Achieving Cyber Essentials Plus

Cyber Essentials Plus goes a step further and actually requires the Certification Body to check your infrastructure for vulnerabilities and ensure that all the answers provided in your SAQ are reflected there. It's important to note that the Plus certification MUST be achieved within 90 days of completing Cyber Essentials Basic.

CYBER ESSENTIALS

Cyber Essentials vs Cyber Essentials Plus

Even by achieving Cyber Essentials Basic, you're taking an important step to show your clients and stakeholders that you care about your cyber security and protecting their data. However, since Cyber Essentials Plus officially verifies this, it is even more impactful. Achieving Plus demonstrates that you are going the extra mile to ensure you handle all your important data in a secure environment.

Cyber Essentials Plus is already required for many government contracts including MOD, and this is likely to increase in the next few years. We recommend that if you do embark on your Cyber Essentials journey, you try and go all the way to Plus to make it really worth your while!

How Much Does Cyber Essentials Cost?

As of January 2022, Cyber Essentials has adapted its pricing to reflect a tiered system based on organisation size.

Micro organisation	0-9 employees	£430+*
Small organisation	10-49 employees	£575+*
Medium organisation	50-249 employees	£650+*
Large organisation	250+ employees	£720 + *

Please note that these prices are a baseline and can differ depending on the Certification Body and their level of service.

*Excludes VAT

What is a Cyber Essentials Plus Pre-Assessment and Why Do You Need It?

For those undertaking the Cyber Essentials Plus certification, we offer a Cyber Essentials Plus with Assured Pass option. This is designed to reassure businesses of a first time pass for the Cyber Essentials Plus certification. This involves unlimited sessions with our assessments team and unlimited vulnerability scanning to confirm alignment with the standard. The Pre-Assessment vulnerability scans are great at highlighting which areas of your cyber security require attention and improvement. They are especially useful as the Cyber Essentials requirements become more challenging.

If you get the all-clear with a pre-assessment vulnerability scan, the final Plus assessment itself really just becomes a formality. You can sit back and relax knowing you'll pass because you've already completed all the necessary remediation. In doing this you'll also avoid any re-certification costs!

> *"...achieving Cyber Essentials Plus just wouldn't have happened without our pre-assessment scan. We had vulnerabilities we didn't even know about but we were able to uncover these during the scans so by the time we got the Plus assessment we felt confident we were going to pass ..."*

What's more, if you know your business has its sights set on Cyber Essentials Plus, you can start the Cyber Essentials Plus vulnerability scanning at the same time as completing your Basic SAQ, taking even more pressure off as you'll have plenty of time to carry out any required remediation.

CYBER ESSENTIALS

What Are the Benefits of Cyber Essentials?

- Cyber Essentials is the only government-backed UK cyber security standard, which means you will be aligning yourself with the most recognised national standard.

- Time. Money. Resources. With a bird's eye view of your cyber security 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.

- If you've always dreamt of landing that HUGE government contract, Cyber Essentials can help you get there. 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.

- Obtaining Cyber Essentials can make a big difference when your organisation is trying to obtain cyber insurance and it is likely that the brokers will be more inclined to offer you a reduced premium as they can see your organisation is cyber safe and making every effort to protect its data. Certifying with us can get you up to 10% off specialist cyber insurance.

- Just as your business provides a service, you are a client to someone else. With that in mind, think how reassured you'd feel if that service was able to demonstrate to you that they care about looking after your data and keeping secure. You'd likely appreciate the work they do even more than you do currently.

  This is the same feeling you want to give to your own clients. You want your clients to appreciate what you do for them and it begins with letting them know that you're making a conscious effort to keep their information protected. Before you know it, you'll have built a huge amount of trust in your client relationships as well as enhanced your reputation in your industry. When your clients are happy, they'll tell people about it - and who knows, those people might just want to come to you for your services too.

CYBER ESSENTIALS

What are the benefits of Cyber Essentials?

There are organisations that simply do not care about cyber security. They believe it is not a priority or even a concern. It’s an unfortunate way of thinking, and one that is unacceptable in this day and age.

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 cyber security. By showcasing the Cyber Essentials logos on your website and collateral, you put your organisation amongst an elite group of organisations in your industry who can demonstrate they care about their data.

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 because the Information Commissioner's Office (ICO) can very quickly conclude that you did not implement enough measures to protect the data you hold. How do they know that? They can see you didn't have Cyber Essentials when you were breached. Simply having the certification could have prevented the fine as they would have been able to see you were trying to protect your data.

How well do 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. The trust gets broken because they won't feel their data is secure with you any longer. With supply chain attacks almost tripling in 2021, managing your cyber risk and ensuring your company is not the reason a supply chain crumbles, is crucial.

With a Cyber Essentials certification, you protect your organisation and your suppliers. You’re also giving them 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

Securing the Supply Chain with Cyber Essentials

Just as those businesses that you supply will want to know you're secure, you'll also want your own suppliers to be secure.

In today's business world, supply chains are no longer linear. We're becoming more digital in the way we work and dealing with suppliers all over the world. This has led to lots of benefits and conveniences, helping to meet the increasing demand of the consumer market, but it has also meant an increase in the cyber threat.

Think about your Supply Chain. How well do you know all your suppliers? Do you really believe that every third-party you work with has adequate cyber security measures in place?

A single vulnerability somewhere in your Supply Chain could allow hackers to access your systems and others' in the same supply chain, which can be catastrophic - just look at the SolarWinds attack in 2020.

If you could have a way to ensure all your suppliers were meeting a good level of cyber security, wouldn't you?

Many companies are already mandating that their suppliers achieve Cyber Essentials in order to work with them for precisely this reason. It's a clear way of demonstrating your level of security so it's easy to check compliance and it's also a clear and tangible security goal for your suppliers.

Our Supply Chain Program is designed to help manage this process. We help identify the right level of Cyber Essentials certification for each supplier depending on their risk and take care of each certification process. You just need to be able to provide at least 10 suppliers for certification and we'll even do your own company's Cyber Essentials certifications for free every year!

CYBER ESSENTIALS

Getting Started with Cyber Essentials: The Controls

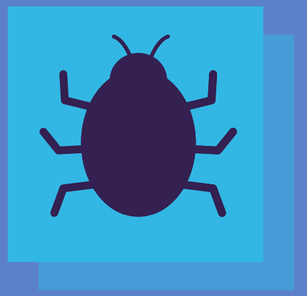
So what is Cyber Essentials actually assessing in order to say that it is confidently protecting your organisation from 80% of the cyber attacks? Well, it seeks to determine whether you are aligned with the five critical controls. You're probably thinking... what on earth is a control? Essentially, technical controls are safeguards that are incorporated into computer hardware, software, or firmware. The controls for Cyber Essentials are:

Access Control
Users should only access the data they really need with correct procedure to deal with admin privileges.

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

Secure Configuration
Avoiding defaults and making sure your settings are correctly configured will make 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 remediated.



Malware Protection
Cyber Essentials checks that you have the appropriate anti-virus protection in place for 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-mails 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 employees 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 emails. Using such accounts in this way exposes the device to compromise by malware. You may not need a technical solution to achieve this if you implement good policy and procedure, alongside 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 (2FA) 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 (2FA) 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 not 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 and as of the 2022 standard, it will now be checked on the Plus assessment that all critical updates with a CVSS (Common Vulnerability Scoring System) score higher than 7.0 are installed within 14 days of release.

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 (7.0+ CVSS) 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 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.

The Cyber Essentials Process

STEP 1: GET IN TOUCH

Give us a call or email to let us know more about your business so we can best advise you on our Cyber Essentials service options. We will need to know how many employees you have at your organisation in order to provide you with an accurate quote.

STEP 2: ACHIEVE CYBER ESSENTIALS (BASIC)

We will grant you access to IASME's portal and guide you through the process of getting your business certified for Cyber Essentials via email or 1-2-1 sessions with an assessor, depending on the level of support you require. The Basic SAQ and review can often take less than 24 hours but don't forget it must be completed within 6 months of you gaining access to the portal. You'll get your logos, certificate and report straight after achieving certification.

STEP 3: CYBER ESSENTIALS PLUS WITH ASSURED PASS

With over 95% of businesses failing Cyber Essentials Plus on their first attempt, we ensure you pass Cyber Essentials Plus first time by highlighting any existing issues so your IT provider can fix them before the actual Cyber Essentials Plus assessment.

STEP 4: ACHIEVE CYBER ESSENTIALS PLUS CERTIFICATION

After all issues are remediated, we will carry out the final Cyber Essentials Plus assessment and once you have officially passed, you'll get your logos, certificate and report.

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.

CYBER ESSENTIALS

Additional FAQs

Does Cyber Essentials expire?

Cyber Essentials does require annual renewal as a lot can change over 12 months so it's necessary to check if you're still compliant.

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, which you must submit within *6 months* of receiving the questionnaire. After completing the Basic, you can work on your Plus and this must be achieved within *3 months* of your Basic being completed, or you will have to start the process again.

How do I become 100% secure?

We'd all love to be 100% secure but unfortunately, this will never be possible. The best thing you can do is guarantee 80% protection from cyber-attacks through Cyber Essentials, and then look to invest in threat detection solutions and continued monitoring to bridge that gap. Cyber insurance is also a must so your assets can be protected should you experience a cyber attack.

My IT team handle my security so why should I bother with Cyber Essentials?

IT teams are of course a great asset to any business, but their main goal is to keep things functioning so your business operations aren't hindered. Cyber security measures on the other hand aim to protect those systems from external attackers and Cyber Essentials outlines the fundamental measures that need to be in place to do that. We work to make sure your business is both functional and secure, and the best starting point is getting your Cyber Essentials certification.

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

This really depends on the size of the company and the complexity of its infrastructure, but it can take as little as 24 hours to achieve Basic. The Plus assessment, which is more extensive, will take longer than this, but if you have the resources to quickly remediate any issues identified, there's no reason you can't secure certification in a short amount of time!

We ensure you have access to the IT support needed for remediation so it doesn't act as a roadblock to certification.

It's your duty to protect your organisation.

The cyber threat is real for every single organisation, whatever the size. With one small business successfully hacked every 19 seconds in the UK, it's up to organisations to do their best to avoid being just another of these statistics and protect their organisation by investing in cyber defences - this starts with Cyber Essentials certifications provided by South West IT. With Cyber Essentials, your organisation can have peace of mind that it's protected against 80% of cyber attacks, as well as reassure your customers and avoid huge fines from the ICO, post-breach.

South West IT LTD
01305 500118
info@sw-it.co.uk

CYBER ESSENTIALS