Guide to **Cyber Essentials**

evalian

This extensive guide will give you a detailed overview of Cyber Essentials and Cyber Essentials Plus. You can use the table of contents in the right-hand sidebar to navigate to different sections.

Introduction

Irrespective of the nature of your organisation, its size, sector and the type of IT used, it is highly likely you use technology that leaves you exposed to hackers. In the same way that you conduct your life with security in mind by repeating behaviours such as locking your front door when you leave the house, or not leaving valuables in an unattended car, cyber security should start with ensuring the basics are done well. This is easy to say, but in practice, much harder to do. The Cyber Essentials standards ensure organisations focus on the basics and the controls in the Cyber Essentials standard are a great starting point. In this guide, we'll address Cyber Essentials and also explain what Cyber Essentials Plus is.

Why is cyber security important for my business?

Before we dive into the 'what' of Cyber Essentials, it's first important to understand the 'why': the value that cyber security brings to your business. Rather than scare you with a long list of hacks, ransomware attacks and data losses, we advocate that you think of cybersecurity as a business enabler. It can be used to foster trust and confidence with existing customers – and can be a differentiator in winning new ones. We're observing many more businesses ask about cyber security in their supply chain and request that their suppliers and partners meet a standard of security. As the tide of cyber security rises, we think it's important your organisation isn't left behind and beached.

Cyber Essentials is a UK Government-backed standard with technical controls recommended from the UK's National Cyber Security Centre (NCSC).

What is the NCSC?

The NCSC is the public-facing part of the Government Communication Headquarters (GCHQ), created in 2016 to help protect the UK's critical services from cyber-attacks, manage major incidents, and improve the underlying security of the UK's Internet through technology improvements and via advice to citizens and organisations. Their vision is to help make the UK the safest place to live and work online.

The NCSC aims to:

- Understand cyber security, and distil this knowledge into practical guidance made available to all;
- Respond to cyber security incidents to reduce the harm they cause to organisations and the wider UK;
- Use industry and academic expertise to nurture the UK's cyber security capability; and
- Reduce risks to the UK by securing public and private sector networks

The NCSC's website is full of great advice for individuals and organisations, however there's so much advice there it's hard to know where to start. We recommend organisations commence their cyber security journey preferably early in their lives and achieve certification against the Cyber Essentials standard. To understand why we recommend this, read a bit more about Cyber Essentials, below.

What is Cyber Essentials?

Cyber Essentials is the NCSC's flagship cyber security standard. As they claim: "Cyber Essentials helps you to guard against the most common cyber threats and demonstrate your commitment to cyber security". The standard was independently reviewed and found to be effective by Lancaster University: "With the CE tools, more than 99% of the vulnerabilities in SMEs interviewed were mitigated".

Whilst the NCSC advertises Cyber Essentials as suitable for any size of organisation, our experience is that it's better suited to small and medium-sized enterprises ("SME"), or organisations with a small IT footprint. Larger and more complex organisations, particularly those with an IT department and/or a risk management function, should look towards the NCSC's 10 Steps, ISO 27001 or the NIST Cyber Security Framework.

Who runs Cyber Essentials and Cyber Essentials Plus?

The NCSC works with IASME to deliver Cyber Essentials.

What is IASME?

IASME is a small British company that provides information assurance and security guidance and standards for small and medium-sized organisations.. After a commercial tender, IASME was chosen by the NCSC to take over full responsibility for Cyber Essentials delivery and from 1st April 2020 became the NCSC's Cyber Essentials Partner. IASME sets the professional requirements for organisations to become a Certification Body, delivers training and ongoing professional education for assessors. IASME sets the questions for Cyber Essentials, and then processes and oversees the quality of the Certifying Bodies' submissions.

We'll now take a look at what you need to do to achieve Cyber Essentials and Cyber Essentials Plus.

What do I do to achieve Cyber Essentials?

Cyber Essentials is easier to achieve than its more demanding sibling (Cyber Essentials Plus), but its focus remains to do the basics to a level that will deter hackers and protect your organisation.

There are five, basic controls to enforce:

1. Use a firewall to secure your Internet connection
2. Choose the most secure settings for your devices and software
3. Control who has access to your data and services
4. Protect yourself from viruses and other malware
5. Keep your devices and software up-to-date

Firewall

First off, all organisations should employ a firewall. For home workers, this isn't an issue as modern routers have a firewall built-in as standard - but it's worth checking with your router provider. You should change the admin password on your router, this is actually much easier to do than you may fear and a quick internet search on this topic should provide an easy how-to-guide that is easy to follow even for those who consider themselves as non-technically adept. Your router is the access portal for data to flow back and forth from your home to the worldwide web. The router is a device that can be accessed from across the world wide web and by changing the admin password you reduce the risk of an attacker being able to log on to that device, update the settings and then dive into the devices which are on your home's network. But make sure your password is a good one – see the excellent guidance here: Three random words or #thinkrandom - NCSC.GOV.UK And we can't emphasise strongly enough that it's worth investing in a password manager.

Secure settings

Ensuring your devices have the most secure settings includes setting up a password or code to access your laptops and mobile phones. Preferably you'll use a biometric access option as this is often more secure and also has a greater degree of convenience for the user. You should also disable or remove any functions, accounts, or services which you do not require – see our comment about 'attack surfaces' below. All your devices and accounts should be password protected, with two-factor authentication (2FA) enabled where possible. 2FA is an effective security measure that often involves a code being sent to your smartphone which you must enter in addition to your password.

Control access

To minimise the potential damage that could be done if an account is accessed by someone else, misused or stolen, staff accounts should have just enough access to software, settings, online services and device connectivity functions for them to perform their role. Extra permissions should only be given to those who need them and only for a limited period. This is an important control because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account. Most devices are delivered with admin accounts as standard and it's quite simple to set up an admin and standard user account on laptops. The standard account should be used for the vast majority of work and, we can't emphasise this enough - by limiting admin access you are greatly increasing the protection afforded to your organisation with little or no cost involved.

Malware protection

We encourage you to protect yourself from viruses and other malware. Malware is short for 'malicious software', that is software specifically designed to disrupt, damage, or gain unauthorised access to a computer system. One specific example is ransomware, which you may have heard of. Ransomware can make your data or systems unusable until you make a payment or perform an action demanded by the attacker. A common approach now is for the attacker to copy your data and then threaten to release it unless a payment is made. Windows has Defender, which is effective enough to pass Cyber Essentials, provided you have enabled its features. Anti-malware features are often included for free in commonly used operating systems and these should be used on all devices.

Patch

Finally, for the love of any otherworldly entity, when your device asks you if you want to close down your programmes, update and restart, do just that. Keeping your operating system up to date is another simple yet outstandingly effective way to protect your organisation. Why? Because when coders write software, they make mistakes. These mistakes sometimes are not realised until the software has been released and is in use by people like you and me. When the mistake has been spotted the software provider releases an update which 'patches' that flaw. The sooner the flaw is patched, the better. So turn on automatic updates, restart all of your devices at least once a week and sensibly dispose of any device which is no longer supported. Cyber Essentials focuses on operating systems rather than device types, so if your device is too old to handle the latest operating software from Microsoft or Google then it's time to upgrade.

What do I do to achieve Cyber Essentials Plus?

Now let's look at the elements of Cyber Essentials Plus which make it more demanding to pass. To achieve Cyber Essentials Plus, an organisation must meet the standard of Cyber Essentials and, in addition, have a vulnerability scan and other technical assessments. These are verified by a Certification Body and you are not able to self-certify.

The additional elements of Cyber Essentials Plus make it a really good standard to adhere to as it checks against several areas which could be exploited by a hacker. These assessments have to be completed by a qualified, third-party Certification Body. Let's look at them in turn.

Vulnerability scans

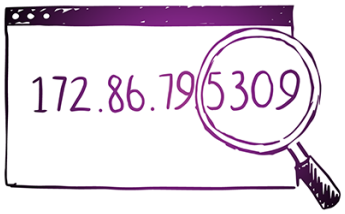
Attack surface

A vulnerability scan is completed using a software tool such as Nessus. This scan will identify any areas of concern. Part of the process of achieving Cyber Essentials is checking what applications you're running and removing any software you don't need. This process reduces what is often termed as the attack surface, as the fewer applications you have, the fewer vulnerabilities should be present. The smaller attack surface you present, the fewer options an attacker has to be successful.

Sample scan

If you can download, install and run Nessus (or other equivalent vulnerability scanning tool) this will give you an idea of the vulnerabilities which exist on your digital estate. By performing a sample scan and ensuring there are no high or critical findings you're in a great position to succeed with the Cyber Essentials Plus assessment. If there are findings, and a patch from the vendor has been made available 14 days prior to testing, there is guidance to assessors concerning the location of the vulnerability and its impact on the success of the assessment.

IP addresses



An IP address (Internet Protocol address) is an identifying number for network hardware connected to a network. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet. For each IP only necessary ports should be opened, traffic to ports not in use should be blocked and no there should be no vulnerabilities scoring above 7 (CVSS 3.0).

Open Ports

A scan of your exterior facing IPs is often the first step in an attack. This type of scan is passive, in that it won't be noticed but it will identify any open ports. Open ports allow data to flow from your devices out to the Internet and vice versa. Only ports which allow essential traffic should be open, open ports that aren't managed enable hackers to gain easy access. Think of these as being like locking your front door, but leaving the patio doors at the back of your house wide open.

Malware protection

If you use an anti-virus, it's essential to ensure it is using the latest version. Many providers of anti-virus software will adapt their product according to the latest threats, so if you're paying for an anti-virus solution you should ensure you benefit from your investment by making sure it is kept up to date. For each device with anti-malware, you need to ensure all definitions are released in the last 24 hours prior to the assessment and all antivirus engines from the last 30 days have been installed.

Email filters

Testing email filters checks to see if executable files can get through to your inbox. Often the settings in your email service help to protect you but these may need to be specifically configured. Your email should not allow files to be opened and run with just one click of your mouse. This is to ensure executable files – the type that carry viruses and malicious code – cannot be easily opened, enabling your staff to be part of your defences. They should know to think before they click.

For your email client(s) you will need to provide a sample test account or a user's account can be used (from the devices provided). For each client, the assessor will send out emails with attachments and for each email, they will need to ensure the attachment does not reach the user. If it does reach the user, it must take at least two clicks to open and execute the attachment.

Web browsers

For each web browser on the laptops assessed the tester will access an URL and attempt to download sample files. When the file is downloaded, the browser must prevent the attachment from being downloaded. Alternatively, it must take more than two clicks to execute the attachment. The easiest way to achieve this will be to enable the "ask where to save each file before downloading" on the browser.

By preventing the attachment from being downloaded straight away you are allowing your staff to think if they really should download this file. Again, this feature can often be adjusted in your browser's settings.

Mobile device protection

You will need to know where your information is flowing and across which devices, so if your staff have work emails on their mobile phones then those devices will automatically fall in the scope of this assessment. They must be running the latest operating software and only use apps from their respective official app stores.

Every mobile phone in the organisation must have the latest OS patches and updates, and the devices must not be rooted or jailbroken. All applications on the devices are to have been installed through the official app store.

Is Cyber Essentials for me?

We consider the Cyber Essentials standards as being suitable for SMEs due to the requirement to patch within 14 days, which can be a bit tricky for larger organisations that have a more complex IT arrangement. We suggest larger organisations implement the NCSC's 10 Steps and plan to achieve ISO27001 or the NIST Cyber Security Framework once it makes business sense to do so. So, if you either have on premises IT, use a cloud service provider, or have a mix of both, Cyber Essentials is a great step towards achieving a security as standard culture in your organisation from the outset.

How do I become Cyber Essentials certified?

Organisations may apply directly for Cyber Essentials, although most use a Certification Body to support their application. Organisations that apply directly will have their application checked by a Certification Body before being awarded Cyber Essentials. A Certification Body is an organisation (like Evalian) that is trained and licenced by IASME to certify to Cyber Essentials or Cyber Essentials Plus. Organisations with a Cyber Essentials certificate are listed on the Cyber Essentials' website, here: https://www.cyberessentials.ncsc.gov.uk/cert-search/

Your 4-steps to Cyber Essentials

We suggest taking the following steps to achieve Cyber Essentials.

1. Conduct the free self-assessment questionnaire, available here. https://getreadyforcyberessentials.iasme.co.uk/questions/
2. Review the results from the questionnaire: we can help with this and advise on achieving Cyber Essentials.
3. Complete our onboarding questionnaire. This will help us define how many hours of work we will need to assess your organisation.
4. Schedule assessment and celebration dates for joining hundreds of other organisations in deterring cyber criminals from accessing your data.

Contact us

Telephone

03330 500 111

Email

hello@evalian.co.uk

Head Office

West Lodge, Leylands Business Park, Colden Common, Hampshire, SO21 1TH

London Office

10 Fitzroy Square, London W1T 5HP

Manchester Office

Jactin House, 24 Hood Street, Ancoats, Manchester, M4 6WX

Dublin Office

69 Main Street, Blackrock, Dublin, Ireland, A94 N6D0

Visit

www.evalian.co.uk