Cyber Essentials

with

Zuri

CYBER ESSENTIALS

IASME CONSORTIUM

CYBER ESSENTIALS PLUS

0204 570 2770
www.zuri-it.com

Introduction

While cyber criminals can and do launch sophisticated, targeted cyber-attacks, the vast majority of threats are basic, opportunistic endeavours that target vulnerabilities wherever they can find them rather than focusing on specific organisations. As the National Cyber Security Centre (NCSC) puts it, these relatively simple methods are "the equivalent of a burglar checking a front door to see if it is locked",[1] and account for around 80% of cyber-attacks.[2]

The **Cyber Essentials scheme** – launched in 2014, backed by the UK government, and most recently updated to v3.1 or 'Montpellier', which came into effect on 24 April 2023 – is designed to help organisations protect themselves from these most common cyber threats, while keeping the approach simple and the costs low. The scheme focuses on **five key cyber security control themes**. Organisations can also achieve Cyber Essentials certification by undergoing an independent assessment to show they are meeting the scheme's requirements.

The benefits of certification

A big benefit of certification – as opposed to merely complying – is that it shows your commitment to cyber security, which in turn will help your business. It reassures customers, partners, regulators and other stakeholders that you are taking security seriously, and are taking reasonable steps to protect their data and ensure service availability. It can also help you appeal to prospects, as well as help you win contracts (or qualify for them in the first place), particularly UK government ones.

However, just implementing the controls offers significant benefits too – for a start, protecting you from the vast majority of attacks. Those attacks may be low-level and easy to execute, but the consequences can be extensive. For instance, Cathay Pacific was fined the maximum amount under the UK's previous, more lenient, data protection law after suffering a breach.[3] Upon investigation, the regulator discovered that the airline failed three Cyber Essentials control themes. It is worth remembering that if you are found to lack even the most basic security, you expose yourself to significantly bigger fines, costlier remediation and harsher criticism that tarnishes your reputation.

Furthermore, achieving certification also qualifies you for reduced insurance premiums. In fact, all UK organisations with an annual turnover below £20 million that achieve Cyber Essentials certification covering the whole organisation can opt in for cyber insurance with a total liability limit of £25,000.[4]

Cyber Essentials has the further benefit that it is a fairly basic framework to implement, making it a good stepping stone for more advanced security frameworks (such as **ISO 27001**), should you decide to implement them at a later stage. Such a move could be motivated by various factors, like a longer-term plan to gradually mature your cyber defences driven by business need, or the intent to tender for bigger, longer-term contracts that demand a higher level of assurance.

Certification scope

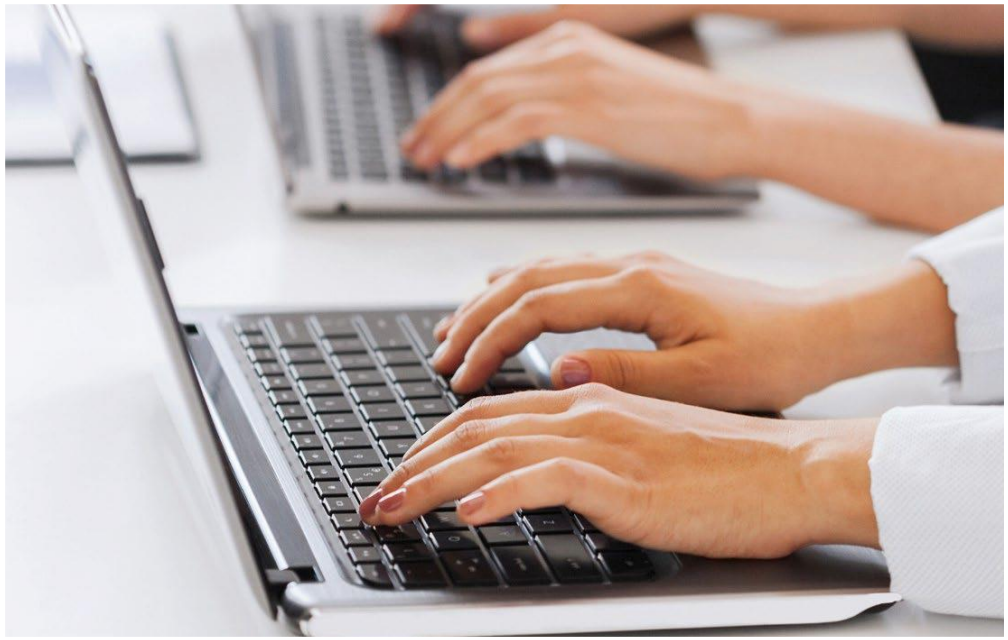
Before starting your assessment, you must agree its scope with your chosen certification body. Ideally, your scope should cover your entire IT infrastructure for the best security and assurance. It is, however, also acceptable to just cover a separately managed subset of your infrastructure, provided that it includes all devices and software that:

- Can accept incoming network connections from the Internet;
- Can establish user-initiated outbound Internet connections; and/or
- Control data flows between the above devices and the Internet.

Whatever your scope, you must clearly define it in terms of the business unit managing it, the network boundary and the physical location.

Asset management

Asset management is a new topic included in the latest version of the scheme, though only as a strong recommendation, not a specific requirement or control. Essentially, it makes the point that good asset management makes managing your cyber security, as well as a range of other business activities, considerably easier. By knowing exactly what your assets are, you also know what you need to protect. This will also help you determine your scope.



The five control themes

To achieve certification, your scope must be covered by the following controls that you can quickly put in place.

1. Firewalls

Cyber Essentials requirement: Every in-scope device must be protected by a correctly configured firewall (or equivalent network device).

Your firewalls work as your gatekeepers: the barriers between your internal network, which needs to remain secure, and the Internet, which should be treated with caution. To be effective, your firewalls must be correctly configured, with those configurations regularly reviewed, and access to the firewall's administrative interface restricted. As part of this, the default administrative password must be changed to a more secure alternative (see 'Password requirements' to the right).

In addition to a boundary firewall for your network, Cyber Essentials requires in-scope devices to use a software firewall.

2. Secure configuration

Cyber Essentials requirement: Actively manage your computers and network devices.

The default configurations on IT equipment and software are often as open as possible for maximum convenience, but this also provides more access points for unauthorised users, which creates more vulnerabilities. With this in mind, Cyber Essentials requires applicants to regularly remove or disable unnecessary services, user accounts and software, as well as disable auto-run features that allow file execution without user authorisation.

In addition, users must change their default or guessable account passwords to more secure alternatives (see 'Password requirements'), and be authenticated before being granted access to organisational data or services.

Finally, devices for which a user needs to be physically present to gain access to the services on that device must be unlocked with a credential such as a password, PIN or biometric authentication factor. Passwords and PINs must contain at least six characters if only used to unlock the device, or meet the scheme's full password requirements if also used elsewhere. Both must be enforced through technical controls, and protected against brute-force attacks (see 'Password requirements' for more detail).

Password requirements

For password-based authentication, Cyber Essentials requires applicants to rely as little as possible on users choosing their own strong passwords, instead using technical controls to enforce at least one of the following for all accounts:

- Multifactor authentication (MFA), with the following conditions:
  - The password element must contain at least eight characters, without any upper limit.
  - The additional authentication factor must be usable and accessible, and be a managed/organisational device, an app on a trusted device, a physically separate token, or a known or trusted account.
- Passwords must contain at least 12 characters, without any upper limit.
- Passwords must contain at least eight characters, without any upper limit, combined with a password blacklist to prevent common passwords from being chosen.

Note, however, that you must implement or use MFA for administrative accounts, for Internet-accessible accounts, and to authenticate to any Cloud services. Cyber Essentials also requires you to protect passwords from brute-force attacks, which you can achieve by using MFA. Alternatively, you can lock accounts after ten or fewer unsuccessful login attempts, or increase the waiting time between login attempts, allowing no more than ten guesses in five minutes.

In addition to these controls, Cyber Essentials requires you to support people in choosing strong, unique passwords and keeping them secure. To an extent, you can achieve this through technical measures by not enforcing complexity requirements or regular password expiry (though you must change passwords as quickly as possible after a known or suspected security compromise).

However, you cannot meet all password requirements through technical controls alone. You must educate your users on how to avoid discoverable passwords – so no pet names, favourite football teams, common keyboard patterns or recycled passwords – and teach them how to choose longer yet memorable passwords.

The latter can be achieved in different ways, such as:

- Promoting good-practice techniques like 'three random words'[5];
- Teaching people how to use password managers; and/or
- Providing physical secure storage, like a locked cabinet.

Although not an explicit Cyber Essentials requirement, an effective way of educating your users is by rolling out basic staff awareness training.

3. Security update management

Cyber Essentials requirement: Keep all in-scope software up to date.

Just setting up and securely configuring your devices and software is not enough to stay protected – it is just as important to regularly update and patch them. Systems running older versions of software, or software that is no longer supported by the developer, are a common factor in many security breaches, as they have known vulnerabilities that criminals frequently exploit. One 2022 report showed that 37% of critical weaknesses in 2021 originated from outdated or vulnerable components, and was also the most common critical weakness in 2019 and 2020.[6] Another report showed that the top vulnerability in 2022 was known vulnerabilities, some as old as from 2017, still being successfully exploited.[7]

To keep your organisation secure, ensure all software is not only supported but also licensed, and removed where this is no longer the case. You should also enable automatic updates where possible, or else ensure updates are applied within 14 days of the vendor releasing them (to balance security with practicality).

4. User access control

Cyber Essentials requirement: Control the user accounts (including those used by third parties) that have access to your organisational data and services by managing access privileges and account authentication.

To ensure only authorised individuals access your devices, applications, servers, accounts, and so on, you must create user accounts with unique credentials, and ensure users are authenticated before granting them access.

Furthermore, those accounts should only have access to what is needed to fulfil the user's role – both in terms of privileges and information – and be password-protected (see **Password requirements**). Limiting access will reduce the impact of an account compromise, should you suffer a security breach.

By the same logic, administrative privileges and accounts should only be granted to people who require them. Even then, those individuals must also be given a standard user account to use for day-to-day work, and only use their administrative privileges when completing administrative tasks. This reduces the risk of an administrative account being compromised.

Cyber Essentials requires user accounts and privileges to be reviewed on a regular basis, and removed or disabled when no longer required.

5. Malware protection

Cyber Essentials requirement: Implement and manage a malware protection mechanism on all in-scope devices.

Malware such as viruses and ransomware can cause significant damage to your IT infrastructure. They often originate from malicious websites and **phishing emails** (where an attacker attempts to trick the recipient into clicking a malicious link or downloading a malicious file).

Implementing technical measures will help mitigate the threat posed by malware. The scheme requires you to correctly implement at least one of the following on every in-scope device, although we recommend implementing both:

1. Anti-malware software

Cyber Essentials requires all in-scope devices to run fully supported anti-malware software that receives regular security updates at a frequency appropriate for the product type and in line with vendor recommendations. The software must be configured to prevent malware from running, malicious code from executing and connections to malicious websites.

2. Whitelisting

Whitelisting involves creating a list of applications permitted on a device, and blocking any application not on that list from running. It is a highly effective and low-maintenance method of preventing unknown applications that may contain malware from running, including malware not detected by anti-malware software. Nevertheless, you must regularly review the list to ensure it stays up to date.

In the case of BYOD, you can make the whitelist available to users, and instruct them to only use the approved applications on the list to access organisational data and/or services.

Whatever measure(s) you choose, we strongly recommend supporting it (or them) with **staff awareness training**. This significantly limits the threat posed by social engineering attacks like phishing, which in turn makes it much less likely for malware to infect your networks.

The certification process

The scheme has two tiers of achievement: Cyber Essentials and Cyber Essentials Plus. All organisations looking to prove their compliance with the scheme need to start with **defining their scope**, then completing a self-assessment questionnaire (SAQ) for Cyber Essentials that is independently verified. Successful applicants will subsequently receive their Cyber Essentials certificate and be added to the IASME database.[8]

Organisations wanting to provide a higher level of assurance that they take security seriously – possibly to meet the prerequisites of a wider range of contracts, including Ministry of Defence ones – can look to also achieve Cyber Essentials Plus certification. It has the same implementation requirements (within your defined scope), but your implementation is verified through a technical audit that must be completed within three months of your basic Cyber Essentials certification.

The technical audit includes a series of internal vulnerability scans and tests of your in-scope systems, which are usually conducted remotely. These tests cover all Internet gateways, and a random, representative sample of internally hosted servers and user devices.

The technical audit concludes with an external vulnerability scan (conducted remotely) of your Internet-facing networks and applications to ensure there are no obvious vulnerabilities. Applicants that pass all elements of the audit are issued their Cyber Essentials Plus certificate, which will again be added to the IASME database.

Why partner with ZURI?

ZURI is a new Managed Service Provider with a team of carefully selected specialists who have extensive technical experience in every aspect of IT and Cybersecurity.

Our experience in working with the Cyber Essentials framework dates back to its inception in 2014. We have helped diverse organisations of all shapes and sizes across multiple sectors, with differing levels of technical maturity, to navigate their initial certification, ongoing compliance and annual recertification.

Zuri has developed the services and processes which deliver the technical controls and compliance that many organisations find difficult or prohibitively expensive to address in-house. These challenges are often magnified in the post-pandemic era, as traditional controls and capabilities have become less effective in managing end user devices as more flexible “work from anywhere” cultures have become widespread.

Regardless of the working model your organisation has adopted - onsite, hybrid or fully remote – Zuri has the experience to help you make the most of your existing investments in IT, and the technology to integrate any additional controls, to ensure certification now and maintain ongoing compliance with the framework.

Our processes ensure the recertification process is kept lean whilst tracking new and emerging requirements of the framework, as it is refined throughout its lifecycle.

We recognise that Cybersecurity spans all aspects of IT but understand that not all aspects of IT apply to all businesses; we therefore work closely with our clients to define bespoke strategies, from the starting line through to certification.

If you would like to have a no-obligation conversation about starting your journey towards certification, please contact me to set up a discovery call at your convenience.

Kind regards

NMacGregor

Neil MacGregor
Director Of Cybersecurity

ZURI

neil@zuri-it.com | 0204 570 2770 | www.zuri-it.com

References

[1] NCSC, “New tool launched to support organisations achieve Cyber Essentials certification”, May 2021, **https://www.ncsc.gov.uk/news/new-tool-to-help-achieve-cyber-essentials-certification**

[2] Department for Business, Innovation & Skills (BIS) et al., “Cyber security boost for UK firms”, January 2015, **https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms**

[3] BBC, “Cathay Pacific fined £500,000 over customer data protection failure”, March 2020, **https://www.bbc.co.uk/news/technology-51736857**

[4] More information is available at: IASME, “Cyber Liability Insurance”, accessed April 2023, **https://iasme.co.uk/cyber-essentials/cyber-liability-insurance**

[5] NCSC, “Top tips for staying secure online – Three random words”, December 2021, **https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words**

[6] Bulletproof, “Bulletproof Annual Cyber Security Industry Report 2022”, March 2022, **https://www.bulletproof.co.uk/industry-reports/bulletproof-annual-cyber-security-report-2022**

[7] Tenable, “Tenable 2022 Threat Landscape Report”, December 2022, **https://www.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report**

[8] A full list of organisations issued their Cyber Essentials and, if applicable, Cyber Essentials Plus certificates within the past 12 months is available at: IASME, “Cyber Essentials Certificate Search”, **https://iasme.co.uk/cyber-essentials/ncsc-certificate-search/**

Note that the database provides information on scope, so covering your whole organisation is a very public and effective means of improving customer (and other stakeholders’) confidence in your security.