Your readiness action plan

Scope of your evaluation

The scope of the CYBER ESSENTIALS (CE) assessment includes the IT infrastructure used to perform your business. This will include all devices that access organisational data and services (including emails), and all cloud services that host organisational data and services.

The preferred answer is for your scope to be “whole organisation” because this gives you the most protection. It will also mean that you qualify for the included cyber liability insurance (if your annual turnover is less than £20 million and you are domiciled in the UK).

In some cases, however, it is not possible to have the whole organisation in scope, for example, if you want to use software that is no longer supported. In this case, you must have a way to separate what is in scope from what is not (e.g. a firewall or a VLAN), and you must be able to clearly describe what the scope is (e.g. our office in Guildford only).

If you have IT equipment that does not ever connect to the internet and does not control data flow to and from the internet, then this is automatically excluded from the scope of CE, and you do not need to declare it.

Please note that if you are a sole trader, your organisation may simply include yourself, your mobile phone and the tools of your trade.

Would this assessment cover the whole of your organisation ?

Yes, this assessment would cover the whole of the organisation

Does the scope of your evaluation include end user devices? (e.g pcs, laptops, tablets and mobile devices that have interfaces used by people)

Yes

Hardware or devices used by your organisation

Hardware and devices are the physical pieces of electronic equipment your organisation owns such as computers, servers, laptops, **thin clients**, printers, tablets and mobile phones.

As well as knowing what physical parts of your organisation are in scope, it is also necessary to know which of your devices or networks (internet connected computers) are in scope.

An important first step is knowing what devices your organisation uses. This section talks about your understanding of what devices you have, where they are, and whether they are supported, maintained, patched and secure.

In addition to having financial worth, devices also hold information, which is valuable to both you and your customers. This might be about your customers, information about your organisation, or emails containing private or confidential information. You can protect your information by ensuring your devices are updated with the latest software, putting access controls in place, using controls to restrict the flow of malware and where appropriate, ensuring that the file system is encrypted (To encrypt files means to turn the information into a code so that unauthorised people cannot read them even if they do intercept them).

So now, in terms of office devices, mobile devices and networking devices, can you list the hardware assets used by your organisation?

Has someone in your organisation a list of all hardware devices that you use. For instance types of laptops, smart phones, firewalls, routers ?

Yes - I have a list of all devices

Do you use thin clients?

No

Do you own or rent servers ?

Yes

Action item

MORE INFO

All servers including virtual servers need to be listed with your other hardware devices.

Software and firmware used by your organisation

If hardware is the physical part of a device, software is the operating system, programs and applications that give the instructions. Firmware is a specific type of software that allows certain pieces of hardware e.g. routers and switches to do what they were designed to do.

Knowing which software and firmware you have and whether they are supported is really important. Software and firmware are supported by the manufacturer for a period of time after they have been developed. This support means that if a mistake or weakness, known as a vulnerability, is discovered in the product, the manufacturer will address it with an update or patch which fixes the problem before it can be exploited by cyber criminals.

A list of software / firmware is sometimes referred to as a software asset list (or inventory). It's good to have a clear picture of what software you have, whether you have got the correct amount of licenses, and whether it is in support (patches are available to fix software vulnerabilities).

Do you have a list of all software / firmware used on devices within your organisation ?

Yes, I hold a list of all software / firmware used on devices within the organisation.

Virtualisation is a technology that allows the hardware of a server to be used to create software-based or 'virtual' versions of computers known as virtual machines.

Virtualisation is made possible with a type of software called a **hypervisor.**

Cloud services are based on the technology of virtualisation. In addition, many organisations use virtualisation to maximize the use of their servers which may be located on site or within data centres.

Do you have any virtualisation infrastructure within your organisation?

No

Do you have automatic update enabled on all your software?

Yes

Do you use software that is no longer in support?

Yes

Action item

IMPORTANT

Think about going through all the software / firmware used within your organisation and ensuring that it is all in support. This might seem like a lot of work, however, in many ransomware attacks out of support software is deliberately targeted by attackers as they know which vulnerabilities are there, and that they will not be fixed. By completing this piece of work, you can look at what software or firmware is not supported and create an action plan to either get software / firmware back into support or update to a more recent supported version.

Have devices that are using unsupported software been moved to a segregated sub-set and internet access removed?

Yes

Boundary devices

Boundary devices are the devices found on the edge of your network. Examples of boundary devices include an office firewall or a broadband router.

Most routers supplied by your Internet Service Provider (ISP) have a firewall built in. Common internet routers are BT Home Hub, Virgin Media Hub or Sky Hub.

Your organisation may also have set up a separate hardware firewall device between your network and the internet. Firewalls are powerful devices, but to be effective they need to be correctly configured.

Smart phones do not come with firewalls as default. A firewall is not necessary on your mobile phone as long as you only allow trusted apps from reputable sources.

Do you have a firewall (or router with a firewall) between your business network and the internet ?

Yes I have some form of protection between the internet and my network

On your firewalls and internet gateways - have you changed all the passwords away from the default passwords and are they difficult to guess and more than 8 characters ?

Yes, I have changed all my passwords to something that is not default and hard to guess

If you thought the passwords were known (someone left and knew the password or something happened like the same password used elsewhere was discovered) would you know when and how to change it ?

Yes, we have a password changing process in place

Accessible services from the internet

Your organisation's devices will connect to the outside, wider internet through a gateway. A gateway in a network has the same job as a gateway in a field. It is there to keep some things in, keep some things out and allow specific things to pass through.

It is important that your gateway doesn’t have holes which could allow things to pass through that you don’t want. Your firewall protects this gateway.

At times your firewall may be configured to open a hole and allow a system on the inside of your network to become accessible from the wider internet (such as a Virtual Private Network server, a mail server or a service that is accessed by your customers). This is sometimes referred to as "opening a port". There are many reasons why you would want to do this and it is possible to do in a secure way, however, there needs to be a valid business requirement to open a port. If this has not been a considered and deliberate decision, it could present a risk to your organisation and the safety of it’s information.

Ensure that there are mechanisms in place to permit only the people who need to access your configuration. For example, the firewall or router might be configured to allow access to an external IP address or range that only your supplier uses, or it might be configured to use two factor authentication. Check with someone in your organisation about whether this applies.

Do you have services enabled that are accessible externally ?

No I dont have services enabled that are accessible externally

Cloud services

Different components of computing are available to users within an organisation remotely over the internet and payable on demand or by subscription. Cloud services is the collective name for these externally manged services. Examples are: Microsoft 365, Dropbox, Googledrive, AWS and Citrix Workspace.

Most organisations use a great many cloud services, it allows for a flexible and collaborative use of a resource without having to make the large outlay for ever changing technology. Cloud computing has revolutionised working models by allowing workers to access and share company information from any location and deliver services online. If workers can access organisation information over the internet from any location, so can criminals, and this has resulted in an increasing number of attacks on cloud services, using techniques to steal user's passwords to access their accounts.

It is crucial that organisations understand their role and responsibilities in the security of the cloud services they use. The five core controls of Cyber Essentials apply to all cloud services.

Do you have a list of all the cloud services you use in your organisation?

Yes

Have you enabled MFA on all accounts to access all the cloud services that you use?

Yes

Have you located and understood the ‘shared responsibility’ security arrangement for each of the cloud services you use?

Yes

Secure configurations

When computers are first set up, they frequently prioritise user ease rather than security.

A typical ‘out-of-the-box’ set-up might enable an administrative account with a standard, publicly known default password. There is often one or more additional user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services, sometimes, even a default file share. All of these present security risks. Like setting sail in a leaky boat, it’s wise to make sure your system is water-tight before you go any further.

Have you been through the devices that you have and disabled the software that you dont use ?

Yes we have disabled the software we dont use

Have you ensured that all the accounts on your devices and cloud services are only those that are used as part of your day to day business ?

Yes we only have accounts on there, which help us with our jobs

Is "AutoRun" or "AutoPlay" disabled on all of your systems ?

Yes, AutoPlay or AutoRun is disabled on all of our systems

For mobile devices, do you set a locking mechanism on your devices to access the software and services installed? This might be a pin number, a password, face-scan or fingerprint.

Yes

Use of Passwords

We need our passwords to be secure and complex so that people cannot guess them to get onto our system.

This section is all about passwords and includes ideas to help ensure that everyone, on every device, employs good password security.

Do you ensure that all default passwords on all devices are changed ?

Yes we change all default passwords

Do you have something written down to advise all users how important it is to use different passwords for different systems?

Yes

Do you make sure that each user requires their own username and password and there are no shared username / passwords?*

Yes, all users require a separate username and password to log onto the systems

Do you have something written down to advise all users about creating good passwords? Does your policy specify the technical controls to manage the quality of passwords used within your organisation? Does the policy include a process for when you believe that a password or an account

has been compromised?

Yes, we have a comprehensive password policy

Is there support in place to help employees choose unique passwords for their work accounts?

Yes

Have you put measures in place to protect accounts against brute-force password guessing?

Yes

Protection against malware

Malware is a shortened form of malicious software. This is software that is designed to steal information, to damage information or to prevent you from delivering information.

One of the ways of protecting your devices and network against malware is to keep your software up-to-date with the latest software patches. An additional method is to ensure that you have antivirus software installed and updating. Antivirus is a commonly used term, but actually combats many types of malware.

• Are all of your computers, your laptops, and your mobile phones protected against malware by using one of these options? (Select the ones that apply.)

- I have anti-virus software installed
- I limit installation of applications to an approved set

Action item

IMPORTANT

Have a look through the options for your antivirus (AV) software and try wherever possible to set it to update (download signatures for AV) at least once per day. Additionally, try and use on-demand file scanning, so all files are scanned before being loaded by applications or the operating system.

MORE INFO

Do you need more information or guidance about malware ? Find out more information **about malware** in our guidance.

Where you use an app store, are users prevented from installing unsigned applications

Yes users can only install signed applications

User accounts

The final part of this assessment is all about how you set up and manage both the user and the administrator accounts.

Is there a process you follow in order to create a new user account?

Yes we have a process which approves creation

Have you a process for tracking user accounts of people who join or leave ?

Yes, there is a process to record all the user accounts we have

Is there a process that is followed before a member of staff is given an administrator account?

Yes, we have rules in place for how administrator accounts are created and how they are used

Do you have a process for ensuring that employees do not use administrator accounts for day to day activities such as browsing the internet and checking emails?

Yes

Backing Up Data

A Cyber Essentials Recommendation

Do you have a system for backing up your organisational data?

Yes

Next steps

For further help and guidance about Cyber Essentials:

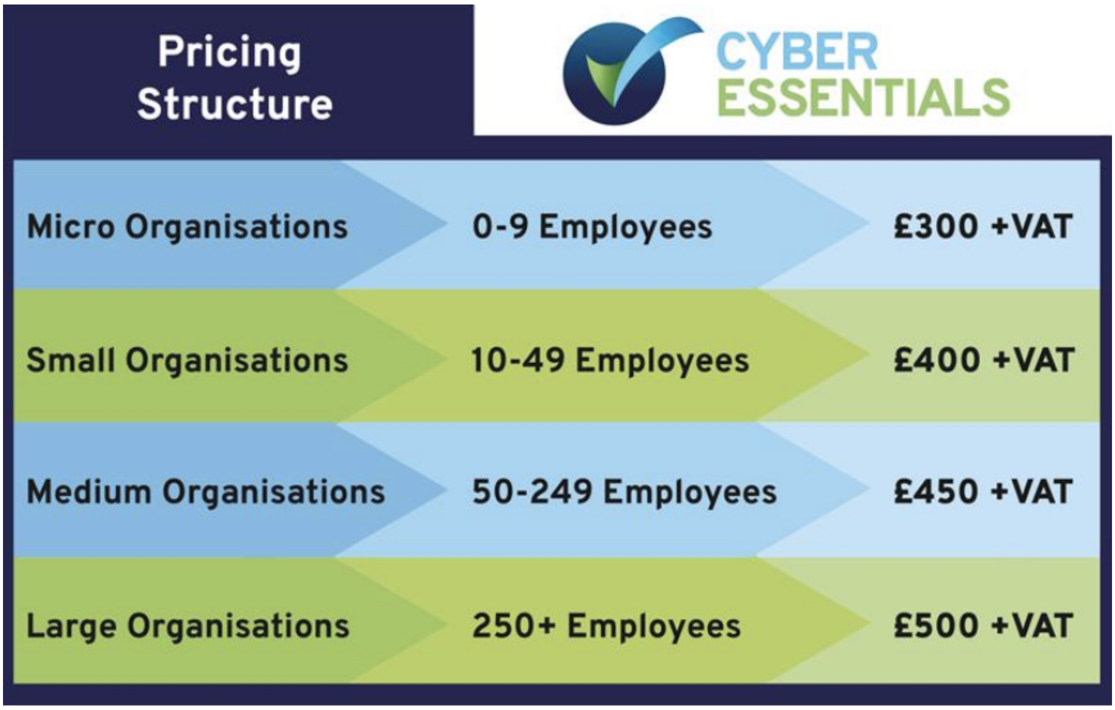
Look through **our frequently asked questions** available on our website.

Join the free Cyber Essentials **LinkedIn advice group here**

The **Cyber Essentials certification bodies** who are located all around the UK and Crown Dependencies are available to offer consulting services to help you achieve your certification.

If you are ready to certify to Cyber Essentials, you can see all the Cyber Essentials assessment questions from **https://iasme.co.uk/cyber-essentials/free-download-of-cyber-essentials-self-assessment-questions/**.

You can apply for a Cyber Essentials assessment via the website **here**. The Cyber Essentials prices can be seen below:.



Pricing Structure

CYBER ESSENTIALS

Micro Organisations	0-9 Employees	£300 +VAT
Small Organisations	10-49 Employees	£400 +VAT
Medium Organisations	50-249 Employees	£450 +VAT
Large Organisations	250+ Employees	£500 +VAT

The benefits of certification

Cyber Essentials can help your organisation in many ways:

- Have the peace of mind that you have implemented the core controls that help prevent most cyber attacks.
- Reassure customers or stake holders that you take cyber security seriously.
- Attract new business and contracts or additional funding and grants that stipulate Cyber Essentials as a prerequisite.
- Be listed on our directory of organisations awarded Cyber Essentials

Readiness tool feedback

We hope you have found this advice tool helpful. We would welcome any feedback to help us improve this tool. To take a short survey please click **here.**