Cyber Essentials Self-Assessment Preparation Booklet

National Cyber Security Centre

Version 15

April 2025

Willow

Introduction

This booklet contains the question set for the Cyber Essentials information assurance standard:

Cyber Essentials

Cyber Essentials is a government-backed scheme focussing on five important technical security controls.

Further guidance on the Cyber Essentials scheme can be found at

https://www.cyberessentials.ncsc.gov.uk

Answering the questions

The booklet is intended to help you to understand the questions and take notes on the current setup in your organisation. In order to complete the assessment, you must enter your answers via IASME's online assessment platform.

You must answer all questions in order to achieve certification.

Your answers must be approved by a Board level representative, business owner or the equivalent, otherwise certification cannot be awarded.

Need help?

If you need help with understanding the questions, get in contact with IASME on +44 (0)3300 882752 or email info@iasme.co.uk

Alternatively, IASME has a network of Certification Bodies who are skilled information assurance companies who can provide advice on the standards and who can help you make changes to your setup in order to achieve compliance. Visit the IASME website at www.iasme.co.uk to find your nearest Certification Body.

Your Company

In this section we need to know a little about how your organisation is set up so we can ask you the most appropriate questions.

A1.1. What is your organisation's name?

The answer given in A1.1 is the name that will be displayed on your certificate and has a character limit of 150 including spaces.

Where an organisation wishes to certify subsidiary companies on the same certificate, the organisation can certify as a group and can include the subsidiaries' name on the certificate as long as the board member signing off the certificate has authority over all certified organisations.

For example:

The Stationary Group, incorporating The Paper Mill and The Pen House

It is also possible to list on a certificate where organisations are trading as other names.

For example:

The Paper Mill trading as The Pen House.

[Notes]

A1.2. What type of organisation are you?

"LTD" – Limited Company (Ltd or PLC)
"LLP" – Limited Liability Partnership (LLP)
"CIC" – Community Interest Company (CIC)
"COP" – Cooperative
"MTL" – Other Registered Mutual (Community Benefit Society, Credit Union, Building Society, Friendly Society)
"CHA" – Registered Charity
"GOV" – Government Agency or Public Body
"SOL" – Sole Trader
"PRT" – Other Partnership
"SOC" – Other Club/ Society
"OTH" – Other Organisation

[Notes]

A1.3. What is your organisation's registration number?

*Please enter the registered number only with **no spaces or other punctuation**. Letters (a-z) are allowed, but you need at least one digit (0-9).*

There is a 20 character limit for your answer.
*If you are applying for certification for more than one registered company, **please still enter only one organisation number**. If you have answered A1.2 with Government Agency, Sole Trader, Other Partnership, Other Club/Society or Other Organisation please enter "none".*
If you are registered in a country that does not issue a company number, please enter a unique identifier like a DUNS number.

[Notes]

A1.4. What is your organisation's address?

Please provide the legal registered address for your organisation.

[Notes]

A1.5. What is your main business?

Please summarise the main occupation of your organisation.

Academia - Pre Schools
Academia - Primary Schools
Academia - Secondary Schools
Academia - Academies
Academia - Colleges
Academia - Universities
Aerospace
Agriculture, Forestry and Fishing
Automotive
Charities
Chemicals
Civil Nuclear
Construction
Consultancy
Defence
Diplomacy
Emergency Services
Energy - Electricity
Energy - Gas
Energy - Oil
Engineering
Environmental
Finance
Food
Government
Health
Hospitality - Food
Hospitality - Accommodation
Hospitality - Hotels
IT
Intelligence
Law Enforcement (Serious & Organised Crime)
Legal
Leisure
Managed Services - IT Managed Services
Managed Services - Other Managed Services
Manufacturing
Media
Membership Organisations
Mining
Other (please describe)
Pharmaceuticals
Political
Postal Services
Property
R&D
Retail
Telecoms
Transport - Aviation
Transport - Maritime
Transport - Rail
Transport - Road
Waste Management
Water
Overseas

[Notes]

A1.6. What is your website address?

Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer.

[Notes]

A1.7. Is this application a renewal of an existing certification or is it the first time you have applied for certification?

If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".

[Notes]

A1.8. What are the two main reasons for applying for certification?

Please let us know the two main reasons why you are applying for certification. If there are multiple reasons, please select the two that are most important to you. This helps us to understand how people are using our certifications.

[Notes]

A1.8.1 Who is the commercial contracting organisation?

Please provide the name of the contracting organisation.

[Notes]

A1.8.2 Who is the commercial contracting organisation?

Please provide the contract number and the contracting organisation.

[Notes]

A1.8.3 Who is the grant authority?

Please provide details of the grant issuing authority.

[Notes]

A1.8.4 Who is the regulator?

Please provide details of the regulator.

[Notes]

A1.8.5 What are the reasons you have applied for the certification which you described as "other"?

Please provide a description.

[Notes]

A1.9. Have you read the 'Cyber Essentials Requirements for IT Infrastructure' document?

Document is available on the NCSC Cyber Essentials website and should be read before completing this question set.
Cyber Essentials Requirements for IT Infrastructure v3.2

[Notes]

A1.10. Can IASME and their expert partners contact you if you experience a cyber breach?

We would like feedback on how well the controls are protecting organisations. If you agree to this then please email security@iasme.co.uk if you do experience a cyber breach. IASME and expert partners will then contact you to find out a little more but all information will be kept confidential.

[Notes]

A1.11. Can IASME contact you for research purposes?

Both IASME and the UK government occasionally need to ask questions about the process and/or benefits of the Cyber Essentials scheme for research purposes. If you agree to this we will contact you via the email address you registered with, you are free to not respond if we do contact you.

Scope of Assessment

In this section, you need to describe the elements of your organisation's IT system that you want to be covered by the Cyber Essentials certification. The scope should be either the whole organisation or an organisational sub-set (for example, the UK operation of a multinational company).

You will also need to answer questions regarding the computers, laptops, servers, mobile phones, tablets, firewalls/routers and cloud services that are connected to the internet and accessing organisational data or services.

All locations that are owned or operated by this organisation or sub-set, whether in the UK or internationally, should be considered "in-scope".

The level of detail required for devices is as follows:
With the exception of network devices (such as firewalls and routers), all other devices within the scope of the certification only need the information about the make and operating system.

The requirement to list the model of the device only applies to question A2.8 in relation to firewalls and routers.

A scope that does not include end user devices is not acceptable.

Further guidance:

Knowledge Hub - Scope

Scope - FAQ

A2.1. Does the scope of this assessment cover your whole organisation? Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to opt in to the included insurance.

Your whole organisation includes all divisions, people and devices which access your organisation's data and services.

About Scope

Subset Scoping Guidance

[Notes]

A2.2. If you are not certifying your whole organisation, then what scope description would you like to appear on your certificate and website?

You will need to have a clear excluding statement within your scope description, e.g. "whole organisation excluding development network".

There is a limit of 300 characters for the scope description on the certificate.

[Notes]

A2.3. Please describe the geographical locations of your business which are in the scope of this assessment.
(e.g. All UK offices) or simply list the locations in scope (e.g. Manchester and Glasgow retail stores).

[Notes]

A2.4. Please list the quantities and operating systems for your laptops, desktops and virtual desktops within the scope of this assessment.

Please Note: You must include make and operating system versions for all devices. All user devices declared within the scope of the certification only require the make and operating system to be listed. We have removed the requirement for you to list the model of the device.

Devices that are connecting to cloud services must be included.

A scope that does not include end user devices is not acceptable.

You need to provide a summary of all laptops, computers, virtual desktops and their operating systems that are used for accessing organisational data or services and have access to the internet.

For example, "We have 25 DELL laptops running Windows 10 Professional version 22H2 and 10 MacBook laptops running MacOS Ventura".

Please note, the edition and feature version of your Windows operating systems are required.
This applies to both your corporate and user owned devices (BYOD).

You do not need to provide serial numbers, MAC addresses or further technical information.

Further guidance:

Operating System Support

Guidance to BYOD

[Notes]

A2.4.1 Please list the quantity of thin clients within the scope of this assessment. Please include make and operating systems.

Please provide a summary of all the thin clients in scope that are connecting to organisational data or services (definitions of which are in the 'Cyber Essentials Requirements for IT Infrastructure' document linked in question A1.9).

Thin clients are commonly used to connect to a Virtual Desktop Solution.

Thin clients are a type of very simple computer holding only a base operating system which are often used to connect to virtual desktops. Thin clients can connect to the internet, and it is possible to modify some thin clients to operate more like PCs, and this can create security complications. Cyber Essentials requires thin clients to be supported and receiving security updates.

Cyber Essentials Requirements for IT Infrastructure v3.2

[Notes]

A2.5. Please list the quantity of servers, virtual servers, virtual server hosts (hypervisors) and Virtual Desktop Infrastructure (VDI) servers. You must include the operating system.

Please list the quantity of all servers within the scope of this assessment.

For example: 2 x VMware ESXI 6.7 hosting 8 virtual Windows 2016 servers; 1 x MS Server 2019; 1 x Red Hat Enterprise Linux 8.3

[Notes]

A2.6. Please list the quantities of tablets and mobile devices within the scope of this assessment.

Please Note: *You must include make and operating system versions for all devices. All user devices within the scope of the certification only require the make and operating system to be listed.*

Devices that are connecting to cloud services must be included.

A scope that does not include end user devices is not acceptable.

Guidance to BYOD

Operating System Support

[Notes]

A2.7. Please provide a list of networks that will be in scope for this assessment.

You should include details of each network used in your organisation including its name, location and its purpose (e.g. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software).

You do not need to provide IP addresses or other technical information.

[Notes]

A2.7.1 How many staff are home or remote workers?

Any employee that has been given permission to work remotely (for any period of time at the time of the assessment) needs to be classed as a home/remote worker for Cyber Essentials.

For further guidance see the Home and remote working section in the Cyber Essentials Requirements for IT Infrastructure document.

Cyber Essentials Requirements for IT Infrastructure v3.2

[Notes]

A2.8. Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers). You must include make and model of each device listed.

You should include all equipment that controls the flow of data to and from the internet. This will be your routers and firewalls.

You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic.

If you have home and/or remote workers they will be relying on software firewalls, please describe in the notes field. You are not required to list any IP addresses, MAC addresses or serial numbers.

[Notes]

A2.9. Please list all of the cloud services that are in use by your organisation and provided by a third party.
Please note that cloud services cannot be excluded from the scope of Cyber Essentials.

You need to include details of all of your cloud services. This includes all types of services - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Definitions of the different types of cloud services are provided in the 'Cyber Essentials Requirements for IT Infrastructure' document.

Cyber Essentials Requirements for IT Infrastructure v3.2

[Notes]

A2.10. Please provide the name and role of the person who is responsible for managing your IT systems in the scope of this assessment.

This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.

[Notes]

Insurance

All organisations with a head office domiciled in the UK and a turnover of less than £20 million can opt into automatic cyber insurance if they achieve Cyber Essentials certification. The insurance is free of charge but you can opt out of the insurance element if you choose. This will not change the price of the assessment package. If you want the insurance then we do need to ask some additional questions and these answers will be forwarded to the broker. The answers to these questions will not affect the result of your Cyber Essentials assessment. It is important that the insurance information provided is as accurate as possible and that the assessment declaration is signed by Board level or equivalent, to avoid any delays to the insurance policy being issued.

A3.1. Is your head office domiciled in the UK or Crown Dependencies and is your gross annual turnover less than £20m?

This question relates to the eligibility of your organisation for the included cyber insurance.

[Notes]

A3.2. If you have answered "yes" to the last question, then your organisation is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element, please opt out here.

There is no additional cost for the insurance. You can see more about it at https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/

[Notes]

A3.3. What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.

The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.

[Notes]

Firewalls

Firewall is the generic name for a piece of software or a hardware device which provides technical protection between your network devices and the Internet, referred to in the question set as boundary firewalls. Your organisation will have physical, virtual or software firewalls at your internet boundaries. Software firewalls are included within all major operating systems for laptops, desktops and servers and need to be configured correctly to provide effective protection.

Questions in this section apply to: boundary firewalls, desktop computers, laptops, routers, servers, IaaS, PaaS, and SaaS.

Further guidance can be found here:

Knowledge Hub - Firewalls

Firewalls - FAQ

A4.1. Do you have firewalls at the boundaries between your organisation's internal networks, laptops, desktops, servers, and the internet?

You must have firewalls in place between your office network and the internet.
CE Requirement: You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).

Further guidance: Firewalls

[Notes]

A4.1.1 Do you have software firewalls enabled on all of your computers, laptops and servers?

Your software firewall needs to be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location.

Guidance on how to check your software firewall can be found here: About Firewalls

CE Requirement: *You must protect every device in scope with a correctly configured firewall (or network device with firewall functionality).*

CE Requirement: *Make sure you use a software firewall on devices which are used on untrusted networks, such as public wifi hotspots.*

If your organisation doesn't control the network to which a device connects, you must configure a software firewall on the device.

[Notes]

A4.1.2 If you answered no to question A4.1.1, is this because software firewalls are not installed by default as part of the operating system you are using? Please list the operating systems.

Only very few operating systems do not have software firewalls available. Examples might include embedded Linux systems or bespoke servers. For the avoidance of doubt, all versions of Windows, macOS and all common Linux distributions such as Ubuntu do have software firewalls available.

[Notes]

A4.2. When you first receive an internet router or hardware firewall device, it may have had a default password on it. Have you changed all the default passwords on your boundary firewall devices?

The default administrator password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (e.g. BT Business Hub, Draytek Vigor 2865ac).

When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.

CE Requirement: *Change default administrative passwords to a strong and unique password – or disable remote administrative access entirely.*

Further guidance: About Routers

[Notes]

A4.2.1 Please describe the process for changing your firewall password?
Home routers not supplied by your organisation are not included in this requirement.

You need to understand how the password on your firewall(s) is changed.

Please provide a brief description of how this is achieved.

[Notes]

A4.3. How is your firewall password configured?

Please select the option being used:

A. Multi-factor authentication, with a minimum password length 8 characters and no maximum length

B. Automatic blocking of common passwords, with a minimum password length 8 characters and no maximum length

C. A password minimum length of 12 characters and no maximum length

D. Passwordless system is being used as an alternative to user name and password, please describe

E. None of the above, please describe

Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document.

Cyber Essentials Requirements for IT Infrastructure v3.2

CE Requirement: *Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:*

- *multi-factor authentication*
- *an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach*

Further guidance : Bulletproof your passwords

[Notes]

A4.4. Do you change your firewall password when you know or suspect it has been compromised?

Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.

When relying on software firewalls included as part of the operating system of your end user devices, the password to access the device will need to be changed.

CE Requirement: *You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.*

Further guidance : Compromised accounts

[Notes]

A4.5. Do you have a process to manage your firewall?

At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks.

[Notes]

A4.6. Have you reviewed your firewall rules in the last 12 months?
Please describe your review process.

If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done?).

CE Requirement: Remove or disable inbound firewall rules quickly when they are no longer needed.

[Notes]

A4.7. Is your firewall configured to allow unauthenticated inbound connections?

By default, most firewalls block all services inside the network from being accessed from the internet, but you need to check your firewall settings.

CE Requirement: *Block unauthenticated inbound connections by default.*

[Notes]

A4.8. Please describe how you approve and document your allowed inbound connections.

The business case should be documented and recorded. A business case must be signed off at board level and associated risks reviewed regularly.

At times your firewall may be configured to allow a system on the inside to become accessible from the internet (for example: a VPN server, a mail server, an FTP server, or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks.

CE Requirement: *Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.*

[Notes]

A4.9. Are your boundary firewalls configured to allow access to their configuration settings over the internet?

Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet.

If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question.

CE Requirement: *Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:*

- *multi-factor authentication*
- *an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach*

Guidance on VPNs

[Notes]

A4.10. If you answered yes in question A4.9, is there a documented business requirement for this access?

When you have made a decision to provide external access to your routers and firewalls, this decision must be documented (for example, written down).

CE Requirement: *Ensure inbound firewall rules are approved and documented by an authorised person, and include the business need in the documentation.*

[Notes]

A4.11. If you answered yes in question A4.9, is the access to your firewall settings protected by either multi-factor authentication or by only allowing trusted IP addresses combined with managed authentication to access the settings?

If you allow direct access to configuration settings via your router or firewall's external interface, this must be protected by one of the two options.

Please explain which option is used.

CE Requirement: *Prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need, and the interface is protected by one of the following controls:*

- *multi-factor authentication*
- *an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach*

[Notes]

Secure Configuration

Computers and cloud services are often not secure upon default installation or setup. An 'out-of-the-box' set-up can often include an administrative account with a standard, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services. All of these present security risks.

Questions in this section apply to: servers, desktop computers, laptops, thin clients, tablets, mobile phones, IaaS, PaaS and SaaS.

Further guidance:

Knowledge Hub - Secure Configuration

Secure configuration - FAQ

A5.1. Where Have you removed or disabled software and services that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services?
Describe how you achieve this.

You must remove or disable applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable any services that are not required for day-to-day use.
To view installed applications:

- *Windows: Right-click on Start > Apps and Features*
- *macOS: Open Finder > Applications*
- *Linux: Open your software package manager (apt, rpm, yum)*

CE Requirement: *You must regularly remove or disable unnecessary software (including applications, system utilities and network services).*
Further guidance : Removing unnecessary software

[Notes]

A5.2. Have you ensured that all your laptops, computers, servers, tablets, mobile devices and cloud services only contain necessary user accounts that are regularly used in the course of your business?

You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services.
To view user accounts:

- *Windows: Right-click on Start > Computer Management > Users*
- *macOS: System Settings > Users and Groups*
- *Linux: "cat/etc/passwd"*

CE Requirement: *You must regularly remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used).*

[Notes]

A5.3. Have you changed the default password for all user and administrator accounts on all your desktop computers, laptops, thin clients, servers, tablets and mobile phones that follow the Password-based authentication requirements of Cyber Essentials?

A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin" or include predictable number sequences such as "12345".

CE Requirement: *You must regularly change any default or guessable account passwords.*
Use technical controls to manage the quality of passwords. This will include one of the following:

- *using multi-factor authentication*
- *a minimum password length of at least 12 characters, with no maximum length restrictions*
- *a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list*

[Notes]

A5.4. Do you run external services that provide access to data (that shouldn't be made public) to users across the internet?

Your business might run software that allows staff or customers to access information across the internet to an external service hosted on the internal network, cloud data centre or IaaS cloud service. This could be a VPN server, a mail server, or an internally hosted internet application such as a SaaS or PaaS cloud service that you provide to your customers as a product. In all cases, these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible.

CE Requirement: *Ensure users are authenticated before allowing them access to organisational data or services.*

[Notes]

A5.5. If yes to question A5.4, which authentication option do you use?

A. Multi-factor authentication, with a minimum password length of 8 characters and no maximum length

B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length

C. A minimum password length of 12 characters and no maximum length

D. Passwordless, please describe

E. None of the above, please describe

Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about 'Password-based authentication' in the 'Cyber Essentials Requirements for IT Infrastructure' document.
Cyber Essentials Requirements for IT Infrastructure v3.2

CE Requirement: *Use technical controls to manage the quality of passwords. This will include one of the following:*

- *using multi-factor authentication*
- *a minimum password length of at least 12 characters, with no maximum length restrictions*
- *a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list*

[Notes]

A5.6. Describe the process in place for changing passwords on your external services when you believe they have been compromised.
Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should know how to change the password if this occurs.

CE Requirement: *You should also make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.*

[Notes]

A5.7. When not using multi-factor authentication, which option are you using to protect your external

The external service that you provide must be set to slow down or stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access.

CE Requirement: *You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following:*

- *'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes*
- *locking devices after more than 10 unsuccessful attempts*

When the vendor doesn't allow you to configure the above, use the vendor's default setting.

[Notes]

A5.8. service from brute force attacks?

A. Throttling the rate of attempts

B. Locking accounts after 10 unsuccessful attempts

C. None of the above, please describe

The external service that you provide must be set to slow down or stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access.

CE Requirement: *You must protect your chosen authentication method (which can be biometric authentication, password or PIN) against brute-force attacks. When it's possible to configure, you should apply one of the following:*

- *'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes*
- *locking devices after more than 10 unsuccessful attempts*
- *When the vendor doesn't allow you to configure the above, use the vendor's default setting.*

[Notes]

A5.9. Have you disabled any feature which allows automatic file execution of downloaded or imported files without user authorisation?

This is a setting on your device which automatically runs software on external media or downloaded from the internet.

It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option, you can answer yes to this question.

CE Requirement: *Disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded).*

[Notes]

Device Locking

A5.10. When a device requires a user to be present, do you set a locking mechanism on your devices to access the software and services installed?

Device locking mechanisms such as biometric, password or PIN, need to be enabled to prevent unauthorised access to devices accessing organisational data or services.

CE Requirement: *Ensure appropriate device locking controls for users that are physically present.*

[Notes]

A5.11. Which method do you use to unlock the devices?

Please refer to Device Unlocking Credentials paragraph found under Secure Configuration in the Cyber Essentials Requirements for IT Infrastructure document for further information.

Cyber Essentials Requirements for IT Infrastructure v3.2

The use of a PIN with a length of at least six characters can only be used where the credentials are just to unlock a device and does not provide access to organisational data and services without further authentication.

CE Requirement: *If a device requires a user's physical presence to access a device's services (such as logging on to a laptop or unlocking a mobile phone), a credential such as a biometric, password or PIN must be in place before a user can gain access to the services.*

You must protect your chosen authentication method against brute-force attacks.

When it's possible to configure, you should apply one of the following:

- *'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt - you shouldn't allow more than 10 guesses in 5 minutes*
- *locking devices after more than 10 unsuccessful attempts*
- *When the vendor doesn't allow you to configure the above, use the vendor's default setting.*

[Notes]

Security update management

rotect your organisation, you should ensure that all your software is always up to date with the latest security updates. If any of your in-scope devices are using an operating system which is no longer supported (for example, Microsoft Windows XP/Vista/2003/Windows 7/Server 2008, MacOS High Sierra, Ubuntu 17.10), and you are not being provided with regular vulnerability fixes from the vendor, then you will not be awarded certification. Mobile phones and tablets are in-scope and must also use an operating system that is still supported by the manufacturer.

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients, mobile phones, routers, firewalls, IaaS and PaaS cloud services.

Further guidance :

Knowledge Hub - Security Update Management

Security Update Management - FAQ

A6.1. Are all operating systems on your devices supported by a vendor that produces regular security updates and vulnerability fixes?

If you have included firewall or router devices in your scope, the firmware of these devices is considered to be an operating system and needs to meet this requirement.

Older operating systems that are out of regular support could be any of the following examples: Windows 7/XP/Vista/ Server 2003, macOS Mojave, iOS 12, iOS 13, Android 8 and Ubuntu Linux 17.10. This is not an extensive list and you should always check with the vendor to confirm if an operating system is still supported

It is important you keep track of your operating systems and understand when they have gone end of life (EOL). Most major vendors will have published EOL dates for their operating systems and firmware.

***CE Requirement:** You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

***Vulnerability fixes** include patches, updates, registry fixes, configuration changes, scripts or any other mechanism approved by the vendor to fix a known vulnerability.*

Further guidance:

Operating System Support
Navigating the pitfalls of legacy software

[Notes]

A6.2. Is all the software on your devices supported by a supplier that produces regular vulnerability fixes for any security problems?

All software used by your organisation must be supported by a supplier who provides regular security updates and vulnerability fixes. Unsupported software must be removed from your devices. This includes frameworks and extensions.

CE Requirement: *You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

[Notes]

A6.2.1 Please list your internet browser(s)
The version is required.

Please list all internet browsers installed on your devices, so that the Assessor can understand your setup and verify that they are in support.

For example: Chrome Version 124, Safari Version 15.

CE Requirement: *You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

[Notes]

A6.2.2 Please list your malware Protection software
The version is required

Please list all malware protection and versions you use so that the Assessor can understand your setup and verify that they are in support.

For example: Sophos Endpoint Protection V10, Microsoft Defender, Bitdefender Internet Security 2023.

CE Requirement: *You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

[Notes]

A6.2.3 Please list your email applications installed on end user devices and server.
The version is required.

Please list all email applications and versions you use so that the Assessor can understand your setup and verify that they are in support.

For example: MS Exchange 2016, Outlook 2019.

CE Requirement: *You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

[Notes]

A6.2.4 Please list all office applications that are used to create organisational data. The version is required

Please list all office applications and versions you use so that the Assessor can understand your setup and verify that they are in support.

For example: MS 365, Libre Office, Google Workspace, Office 2016.

CE Requirement: *You must make sure that all software in scope is kept up to date. All software on in-scope devices must be licensed and supported.*

[Notes]

A6.3. Are any of the in-scope software or cloud services unlicensed or unsupported?

All software must be licensed. It is acceptable to use free and open-source software as long as you comply with any licensing requirements.

Please be aware that for some operating systems, firmware and applications, if annual licensing is not purchased, they will not be receiving regular security updates.

CE Requirement: *All software on in-scope devices must be licensed and supported.*

[Notes]

A6.3.1 If yes to A6.3, please list the unsupported or unlicensed software or cloud services.

[Notes]

A6.4. Are all high-risk or critical security updates and vulnerability fixes for operating systems and router and firewall firmware installed within 14 days of release?

You must install all high and critical security updates and vulnerability fixes within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement.

This requirement includes the firmware on your firewalls and routers.

***CE Requirement:** All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:*

- *The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'*
- *The update addresses vulnerabilities with a CVSSv3 base score of 7 or above*
- *There are no details of the level of vulnerabilities the update fixes provided by the vendor*

Please note: For optimum security we strongly recommend (but it's not mandatory) that all released updates are applied within 14 days of release.

It's important that updates are applied as soon as possible. 14 days is considered a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.

[Notes]

A6.4.1 Are all updates applied for operating systems by enabling auto updates?

Most devices have the option to enable auto updates. This must be enabled on any device where possible.

***CE Requirement:** All software on in-scope devices must have automatic updates enabled where possible.*

[Notes]

A6.4.2 Where auto updates are not being used, how do you ensure all high-risk or critical security updates and vulnerability fixes of all operating systems and firmware on firewalls and routers are applied within 14 days of release?

Please It is not always possible to apply auto updates, this is often the case when you have critical systems or servers and you need to be in control of the updating process.

Please describe how any updates are applied when auto updates are not configured.

If you only use auto updates, please confirm this in the notes field for this question.

CE Requirement: *All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:*

- *The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'*
- *The update addresses vulnerabilities with a CVSSv3 base score of 7 or above*
- *There are no details of the level of vulnerabilities the update fixes provided by the vendor*

[Notes]

A6.5. Are all high-risk or critical security updates and vulnerability fixes for applications (including any associated files and extensions) installed within 14 days of release?

You must install any such updates and vulnerability fixes within 14 days in all circumstances.

If you cannot achieve this requirement at all times, you will not achieve compliance to this question.

You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.

CE Requirement: *All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:*

- *The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'*
- *The update addresses vulnerabilities with a CVSSv3 base score of 7 or above*
- *There are no details of the level of vulnerabilities the update fixes provided by the vendor*

[Notes]

A6.5.1 Are all updates applied on your applications by enabling auto updates?

Most devices have the option to enable auto updates. Auto updates should be enabled where possible.

CE Requirement: *All software on in-scope devices must have automatic updates enabled where possible.*

[Notes]

A6.5.2 Where auto updates are not being used, how do you ensure all high-risk or critical security updates of all applications are applied within 14 days of release?

It is not always possible to apply auto updates, this is often the case when you have critical systems or applications and you need to be in control of the updating process.

Please describe how any updates and vulnerability fixes are applied when auto updates are not configured.

If you only use auto updates, please confirm this in the notes field for this question.

CE Requirement: *All software on in-scope devices must be updated, including vulnerability fixes, within 14 days of release, where:*

- *The update fixes vulnerabilities described by the vendor as 'critical' or 'high-risk'*
- *The update addresses vulnerabilities with a CVSSv3 base score of 7 or above*
- *There are no details of the level of vulnerabilities the update fixes provided by the vendor*

[Notes]

A6.6. Have you removed any software installed on your devices that is no longer supported and no longer receives regular updates or vulnerability fixes for security problems?

You must remove older software from your devices when it is no longer supported by the manufacturer. Such software might include older versions of web browsers, operating systems, and all application software.

CE Requirement: *All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet.*

[Notes]

A6.7. Where you have a business need to use unsupported software, have you moved the devices and software out of scope of this assessment? Please explain how you achieve this.

Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set with no internet access.

If the out-of-scope sub-set remains connected to the internet, you will not be able to achieve whole company certification and an excluding statement will be required in question A2.2.

A sub-set is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.

Where no unsupported software is used across your whole organisation, please declare this here.

***CE Requirement:** All software on in-scope devices must be removed from devices when it becomes unsupported, or removed from scope by using a defined sub-set that prevents all traffic to/from the internet.*

Further guidance: Subset Scoping Guidance

[Notes]

User 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.

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients, mobile phones, IaaS, PaaS and SaaS

Further guidance :

Knowledge Hub - User Access Control

User Access Control - FAQ

A7.1. Are your users only provided with user accounts after a process has been followed to approve their creation? Describe the process.

You must 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 the business.

CE Requirement: *Your organisation must have in place a process to create and approve user accounts.*

[Notes]

A7.2. Are all your user and administrative accounts accessed by entering unique credentials?

You must ensure that no devices, applications or cloud services can be accessed without entering unique access credentials.

Accounts must not be shared.

CE Requirement: *Authenticate users with unique credentials before granting access to applications or devices.*

[Notes]

A7.3. How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?

When an individual leaves your organisation, you need to stop them accessing any of your systems.

CE Requirement: *Remove or disable user accounts when no longer required.*

[Notes]

A7.4. Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?

When a staff member changes job role you may also need to change their permissions to only access the files, folders and applications that they need to do their day-to-day work.

For Cyber Essentials we require that the principle of least privilege be applied.

CE Requirement: *Your organisation must be in control of your user accounts and the access privileges that allow access to your organisational data and services.*

[Notes]

Administrative Accounts

User accounts with special access privileges (e.g. administrative accounts) typically have the greatest level of access to information, applications and computers. When these privileged accounts are accessed by attackers they can cause the most amount of damage because they can usually perform actions such as install malicious software and make changes. Special access includes privileges over and above those of normal users.

It is not acceptable to work on a day-to-day basis in a privileged “administrator” mode.

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients, mobile phones, IaaS, PaaS and SaaS

A7.5. Do you have a formal process for giving someone access to systems at an “administrator” level and can you describe this process?

You must have a process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.

CE Requirement: *Your organisation must have in place a process to create and approve user accounts.*

[Notes]

A7.6. How does your organisation make sure that separate accounts are used to carry out administrative tasks (such as installing software or making configuration changes)?

You must use a separate administrator account from the standard user account, when carrying out administrative tasks such as installing software. Using administrator accounts all day long exposes the device to compromise by malware.

Cloud service administration must be carried out using separate accounts.

Further guidance:
User Access - Just Enough or Just In Time

CE Requirement: *Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).*

[Notes]

A7.7. How does your organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email?

This question relates to the activities carried out when an administrator account is in use.

You must 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. Software and update downloads should be performed as a standard user and then installed as an administrator. You may not need a technical solution to achieve this, it could be based on good policy, procedure and regular training for staff.

CE Requirement: *Your organisation must use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks).*

[Notes]

A7.8. Do you formally track which users have administrator accounts in your organisation?

You must track all people that have been granted administrator accounts.

CE Requirement: *Your organisation must have in place a process to create and approve user accounts.*

[Notes]

A7.9. Do you review who should have administrative access on a regular basis?

You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.

CE Requirement: *Your organisation must remove or disable special access privileges when no longer required (when a member of staff changes role, for example).*

[Notes]

Password-Based Authentication

All accounts require the user to authenticate. Where this is done using a password the following protections should be used:

- Passwords are protected against brute-force password guessing.
- Technical controls are used to manage the quality of passwords.
- People are supported to choose unique passwords for their work accounts.
- There is an established process to change passwords promptly if the applicant knows or suspects the password or account has been compromised.

Further guidance: The Value of Passwords

A7.10. Where you have systems that require passwords (or where passwords are a backup for a passwordless system), how are they protected from brute-force attacks?

A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

Information on how to protect against brute-force password guessing can be found in the Password-based authentication section, under the User Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure' document.

Cyber Essentials Requirements for IT Infrastructure v3.2

CE Requirement: *Passwords are protected against brute-force password guessing by implementing at least one of:*

- *multi-factor authentication*
- *'throttling' the rate of attempts, so that the length of time the user must wait between attempts increases with each unsuccessful attempt – you shouldn't allow more than 10 guesses in 5 minutes*
- *locking devices after no more than 10 unsuccessful attempts*

[Notes]

A7.11. Which technical controls are used to manage the quality of your passwords within you organisation?

Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document.

Cyber Essentials Requirements for IT Infrastructure v3.2

CE Requirement: *Use technical controls to manage the quality of passwords. This will include one of the following:*

- *using multi-factor authentication*
- *a minimum password length of at least 12 characters, with no maximum length restrictions*
- *a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.*

[Notes]

A7.12. Please explain how you encourage people to use unique and strong passwords.

You need to support those that have access to your organisational data and services by informing them of how they should pick a strong and unique password.

Further information can be found in the Password-based authentication section, under the User Access Control section in the Cyber Essentials Requirements for IT Infrastructure document.

Cyber Essentials Requirements for IT Infrastructure v3.2

CE Requirement: *Support users to choose unique passwords for their work accounts by:*

- *educating people about avoiding common passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers*
- *encouraging people to choose longer passwords by promoting the use of multiple words (a minimum of three) to create a password (such as the NCSC's guidance on using three random words)*
- *providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used*
- *not enforcing regular password expiry*
- *not enforcing password complexity requirements*

[Notes]

A7.13. Do you have a process for when you believe the passwords or accounts have been compromised?

You must have an established process that details how to change passwords promptly if you believe or suspect a password or account has been compromised.

CE Requirement: *You should make sure there is an established process in place to change passwords promptly if you know or suspect a password or account has been compromised.*
Further guidance: Compromised accounts

[Notes]

A7.14. Do all of your cloud services have multi-factor authentication (MFA) available as part of the service?

Where your systems and cloud services support multi-factor authentication (MFA), for example, a text message, a one-time access code, notification from an authentication app, then you must enable this for all users and administrators. For more information see the NCSC's guidance on MFA at Multi-factor authentication for online services

Where a cloud service does not have its own MFA solution but can be configured to link to another cloud service to provide MFA, the link will need to be configured.

A lot of cloud services use another cloud service to provide MFA. Examples of cloud services that can be linked to are Azure, MS365, Google Workspace.

***CE Requirement:** Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.*

Further guidance:
Applying MFA to access cloud services
Securing Your Cloud Services

[Notes]

A7.15. If you have answered 'No' to question A7.14, please provide a list of your cloud services that do not provide any option for MFA.

You must provide a list of cloud services that are in use by your organisation that do not provide any option for MFA.

[Notes]

A7.16. Has MFA been applied to **all** administrators of your cloud services?

It is required that all administrator accounts on cloud service must apply multi-factor authentication in conjunction with a password of at least 8 characters.

***CE Requirement:** Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.*

[Notes]

A7.17. Has MFA been applied to **all** users of your cloud services?

All users of your cloud services must use MFA in conjunction with a password of at least 8 characters.

***CE Requirement:** Your organisation must implement MFA, where available – authentication to cloud services must always use MFA.*

[Notes]

Malware protection

Malware (such as computer viruses) 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. Anti-malware solutions (including anti-virus) are available from commercial suppliers, some free, but usually as complete software and support packages.

Malware is continually evolving, so it is important that the supplier includes detection facilities which are updated as frequently as possible. Anti-malware products can also help confirm whether websites you visit are malicious.

Questions in this section apply to: servers, desktop computers, laptops, tablets, thin clients, mobile phones, IaaS, PaaS and SaaS

Further guidance :

Knowledge Hub - Malware Protection

Malware Protection - FAQ

A8.1. Are all of your desktop computers, laptops, tablets and mobile phones protected from malware by either:

A – Having anti-malware software installed

And/or

B – Limiting installation of applications by application allow listing (For example, using an app store and a list of approved applications, using a Mobile Device Management(MDM solution))

or

C – None of the above, please describe

Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B.

Option A - option for all in-scope devices running Windows or macOS including servers, desktop computers, laptop computers

Option B - option for all in-scope devices

Option C - none of the above, explanation notes will be required.

CE Requirement: *You must make sure that a malware protection mechanism is active on all devices in scope. For each device, you must use at least one of the options listed below.*

- *Anti-malware software (option for in-scope devices running Windows or MacOS including servers, desktop computers, laptop computers)*
- *Application allow listing (option for all in-scope devices). Only approved applications, restricted by code signing, are allowed to execute on devices.*

[Notes]

A8.2. If Option A has been selected: Where you have anti-malware software installed, is it set to update in line with the vendor's guidelines and prevent malware from running on detection?

This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-malware software. You can use any commonly used anti-malware product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose.

CE Requirement: *If you use anti-malware software to protect your device it must be configured to:*

- *be updated in line with vendor recommendations*
- *prevent malware from running*
- *prevent the execution of malicious code*

[Notes]

A8.3. If Option A has been selected: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?

Your anti-malware software or internet browser should be configured to prevent access to known malicious websites. On Windows 11, MS Defender SmartScreen can provide this functionality.

CE Requirement: *If you use anti-malware software to protect your device it must be configured to:*

- *prevent connections to malicious websites over the internet.*

[Notes]

A8.4. If Option B has been selected: Where you use an app-store or application signing, are users restricted from installing unsigned applications

Some operating systems which include Windows, Chromebooks, mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.

CE Requirement: *Only approved applications, restricted by code signing, are allowed to execute on devices.*

[Notes]

A8.5. If Option B has been selected" Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you maintain this list of approved applications?

You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use Mobile Device Management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, processes and training of staff.

CE Requirement:

- *actively approve such applications before deploying them to devices*
- *maintain a current list of approved applications, users must not be able to install any application that is unsigned or has an invalid signature*

[Notes]

Achieving compliance with the Cyber Essentials profile indicates that your organisation has taken the steps set out in the HMG Cyber Essentials Scheme documents. It does not amount to an assurance that the organisation is free from cyber vulnerabilities and neither IASME Consortium Limited nor the Certification Body accepts any liability to certified organisations or any other person or body in relation to any reliance they might place on the certificate.