# Cyber Essentials
# Self-Assessment Preparation Booklet

Assured Service Provider

in association with
National Cyber Security Centre

Version 13

November 2021

Evendine

## 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 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 you 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 (for companies: as registered with Companies House)?

*Please provide the full registered name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity as per Companies House registration.*
*Certification should cover one organisation; there are occasions when a certificate can be issued to more than one company. This will be determined by the IT infrastructure. An example would be where all the companies within a company group share the same IT infrastructure.*

*If a client requires certification for a company that has more than one subsidiary registered with Companies House under different names and registration numbers, as long as they share the same network boundary, they can all be entered within one certificate.*

*For example: The Stationery Group, incorporating subsidiaries, The Paper Mill and The Pen House.*
*Adding a trading name to the certification: If an organisation operates under a different trading name to the registered company name, this may also be entered. For example: registered company trading as Company Y.*
*The answer provided to A1.1 will be used to generate the CE certificate.*

[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 (if you have one)?

*If you are a UK limited company, your registration number will be provided by Companies House, in the Republic of Ireland, this will be provided by Companies Registration Office. Charities, partnerships, and other organisations should provide their registration number if applicable.*
*If a client is applying for certification for more than one registered company, just one registration number can be entered to represent the entire group.*

[Notes]

A1.4. What is your organisation's address (for companies: as registered with Companies House)?
***Please provide the legal registered address for your organisation, if different from the main operating location.***

[Notes]

A1.5. What is your main business?
***Please summarise the main occupation of your organisation.***

Agriculture, Forestry and Fishing

Mining and Quarrying

Manufacturing

Electricity, Gas, Steam and Air-conditioning Supply

Water supply, Sewerage, Waste management and Remediation

Construction

Wholesale and Retail trade

Repair of motorcars and motorcycles

Transport and storage

Accommodation and food services

Information and communication

Financial and insurance

Real estate

Professional, scientific, and technical

Administration and support services

Public administration and defence

Compulsory social security

Education

Human Health and Social Work

Arts Entertainment and Recreation

Other service activities

Activities of households as employers; undifferentiated goods and services producing for households for own use

Activities of extraterritorial organisations and bodies

[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. How many staff are home workers?

*Any employee contracted or legally required to work at home for any period of time at the time of the assessment, needs to be classed as working from home for Cyber Essentials.*

[Notes]

A1.8. Is this application a renewal of an existing certification or is it the first time you have applied for certification?

*The Cyber Essentials certification requires annual renewal. If you have previously achieved Cyber Essentials, please select "Renewal". If you have not previously achieved Cyber Essentials, please select "First Time Application".*

[Notes]

A1.9. What is your main reason for applying for certification?

*Please let us know the main reason why you are applying for certification. If there are multiple reasons, please select the one that is most important to you. This helps us to understand how people are using our certifications. (If your reason for certifying is for a government contract, please provide the contract or framework name. This information is helpful to us, but you are not required to provide it).*

[Notes]

A1.10. 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. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

[Notes]

# Scope of Assessment

In this section, we need you to describe the elements of your organisation which you want to certify to this accreditation. The scope should be either the whole organisation or an organisational sub-unit (for example, the UK operation of a multinational company). All computers, laptops, servers, mobile phones, tablets, and firewalls/routers that can access the internet and are used by this organisation or sub-unit to access organisational data or services should be considered "in-scope". All locations that are owned or operated by this organisation or sub-unit, whether in the UK or internationally should be considered "in-scope". A scope that does not include user devices is not acceptable.

The scoping requirements have been updated to include cloud services. More information can be found in the 'Cyber Essentials requirement for Infrastructure v3.0' document. Link is referenced in question A1.11.

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 apply for insurance.*
***Your whole organisation would include all divisions and all people and devices that use business data.***

[Notes]

A2.2. If it is not the whole organisation, then what scope description would you like to appear on your certificate and website?
***Your scope description should provide details of any areas of your business that have internet access and have been excluded from the assessment (for example, "whole organisation excluding development network").***

[Notes]

A2.3. Please describe the geographical locations of your business which are in the scope of this assessment.
***You should provide either a broad description (i.e., All UK offices) or simply list the locations in scope (i.e., Manchester and Glasgow retail stores).***

[Notes]

A2.4. Please list the quantities of laptops, desktops and virtual desktops within the scope of this assessment. You must include model and operating system version for all devices. For Windows devices the Edition and Feature version are also required. All devices that are connecting to cloud services must be included.

*Please provide a summary of all laptops, computers and virtual desktops that are used for accessing organisational data or services and have access to the internet (for example, "We have 25 DELL Vostro 5510 laptops running Windows 10 Professional version 20H2 and 10 MacBook Air laptops running MacOS Big Sur"). This applies to both corporate and personal devices (BYOD). You do not need to provide serial numbers, mac addresses, or further technical information.*

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

| [Notes] |
|---|

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

This question is currently for Information only. From January 2023 this question will require that your thin clients are supported and receiving security updates and will be marked for compliance. thin clients are currently in scope for all other controls.

*Please provide a summary of all the thin clients in scope that are connecting to the organisational data for services. (Definitions of which are in the 'CE Requirements for Infrastructure document' located here https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

| [Notes] |
|---|

A2.5. Please list the quantities of servers, virtual servers, and virtual server hosts (hypervisor). You must include the operating system.

*Please list the quantity of all servers within 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 Redhat Enterprise Linux 8.3.*

| [Notes] |
|---|

A2.6. Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system versions for all devices. All devices that are connecting to cloud services must be included.

*All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. This applies to both corporate and personal owned devices (BYOD). You do not need to provide serial numbers, mac addresses, or other technical information. All tablets and mobile devices connecting to cloud services cannot be excluded from the scope of certification.*

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

| [Notes] |
|---|

A2.7. Please provide a list of the networks that will be in the scope for this assessment.
*You should include details of each network used in your organisation including its name, location, and its purpose (i.e., Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software, (home workers network - based in UK). You do not need to provide IP addresses or other technical information.*

*You should also summarise any home-workers and include their internet boundary that will be taken into consideration for the assessment.*

*For further guidance see the Home Working section in the 'CE Requirements for Infrastructure Document'.*
*https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

| [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 such as 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. You do not need to provide IP addresses, MAC addresses or serial numbers.*

| [Notes] |
|---|

A2.9. Please list all cloud services that are provided by a third party and used by your organisation.
*You need to include details of all your cloud services. This includes all types of services – IaaS, PaaS, and SaaS. Definitions of the different types of cloud services are provided in the 'CE Requirements for Infrastructure Document'.*

***Please note cloud services cannot be excluded from the scope of CE.***

| [Notes] |
|---|

A2.10. Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment?
*This should be the person who influences and makes decisions about the computers, laptops, servers, tablets, mobile phones, and network equipment within your organisation. 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 get 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 a senior person at Board level or equivalent, to avoid any delays to the insurance policy being issued.**

A3.1. Is your head office domiciled in the UK 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 your total gross revenue? Please provide figure to the nearest £100K. 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. Please be as accurate as possible - figure should be to the nearest £100K.*

| [Notes] |
|---|

A3.4. Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? 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.*

| [Notes] |
|---|

A3.5. Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA?

*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.*

| [Notes] |
| --- |

A3.6. 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] |
| --- |

# Office Firewalls and Internet Gateways

**Firewall is the generic name for a software(host-based) or hardware device which provides technical protection between your networks and devices and the Internet, referred to in the question set as boundary firewalls. Your organisation will have a physical, virtual or software firewall at the internet boundary. Software firewalls are also included within all major operating system for laptops, desktops and servers. Firewalls are powerful physical, virtual or software devices, which need to be configured correctly to provide effective security.**

**Questions in this section apply to: boundary firewalls, routers, computers, laptops and servers.**

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.*

| [Notes] |
|---|

A4.1.1 When corporate or user-owned devices (BYOD) are not connected to the organisation's internal network, how are the firewall controls applied?
*You should also have firewalls in place for home-based workers, if those users are not using a corporate Virtual Private Network (VPN) connected to your office network, they will need to rely on the software firewall included in the operating system of the device in use.*

| [Notes] |
|---|

A4.2. When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices?
*The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Business Hub, Draytek Vigor 2865ac).*

| [Notes] |
|---|

A4.2.1 Please describe the process for changing the firewall password.
*You need to be aware of how the password on the firewall is changed. Please give brief description of how this is achieved.*

| [Notes] |
|---|

A4.3. Is the new password configured to meet the Password-based authentication requirements? Please select the option being used

A. Multi-factor authentication, with a minimum password length of 8 characters and no max length.
B. Automatic Blocking of common passwords, with minimum password length of 8 characters and no maximum length.
C. A password minimum length of 12 characters and no maximum length.

*Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

[Notes]

A4.4. Do you change the 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 on end user devices the password to access the device will need to be changed.*

[Notes]

A4.5. Do you have any services enabled that can be accessed externally from your internet router, hardware firewall or software 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. If you have not enabled any services, answer "No". By default, most firewalls block all services.*

[Notes]

A4.5.1 Do you have a documented business case for all of these services?

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

[Notes]

A4.6. If you do have services enabled on your firewall, do you have a process to ensure they are disabled in a timely manner when they are no longer required? A description of the process is required.

*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).*

| [Notes] |
|---|

A4.7. Have you configured your boundary firewalls so that they block all other services from being advertised to the internet?

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

| [Notes] |
|---|

A4.8. 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.*

| [Notes] |
|---|

A4.9. If yes, is there a documented business requirement for this access?

*You must have made a decision in the business that you need to provide external access to your routers and firewalls. This decision must be documented (i.e., written down).*

| [Notes] |
|---|

A4.10. If yes, is the access to the settings protected by either multi-factor authentication or by only allowing trusted IP addresses combined with managed authentication settings? Please explain which option is used.

*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.*

| [Notes] |
|---|

A4.11. Do you have software firewalls enabled on all of your desktop computers, laptops and servers?
*Your software firewall must be configured and enabled at all times, even when sitting behind a physical/virtual boundary firewall in an office location. You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for "Windows firewall". On Linux try "ufw status".*

| [Notes] |
|---|

A4.12. If no, is this because software firewalls are not installed by default for 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] |
|---|

# Secure Configuration

**Computers are often not secure upon default installation. 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.

A5.1. Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, desktop computers, thin clients, servers, tablets, mobile phones and cloud services? Describe how you achieve this.
*To view your installed applications on Windows, look in Start Menu, on macOS open Finder -> Applications and on Linux open your software package manager (apt, rpm, yum). You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use. You need to check your cloud services and disable and services that are not required for day-to-day use*

| [Notes] |
|---|

A5.2. Have you ensured that all your laptops, computers, servers, tablets, and mobile devices 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. You can view your user accounts on Windows by righting-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using "cat /etc/passwd"*

| [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".*

| [Notes] |
|---|

A5.4. Do you run external services that provides 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 or cloud data centre. This could be a VPN server, a mail server, or an internet application (SaaS or PaaS) 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.*

| [Notes] |
|---|

A5.5. If yes, which option of password-based authentication 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 password with a minimum length of 12 characters and no maximum length.

*Acceptable technical controls that you can use to manage the quality of your passwords are outlined in the new section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

| [Notes] |
|---|

A5.6. Describe the process in place for changing passwords 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 be aware of this and know how to change the password if this occurs.*

| [Notes] |
|---|

A5.7. When not using multi-factor authentication which option are you using to protect your external service from brute force attacks?

*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.*

| [Notes] |
|---|

A5.8. Do you have a documented password policy that guides all users of the external service?
*The password policy must include: guidance on how to use longer passwords, for example 'Three Random Words', not to use the same password for multiple accounts, which passwords may be written down and where they can be stored, and if they may use a password manager.*

| [Notes] |
| --- |

A5.9. Is "auto-run" or "auto-play" disabled on all of your systems?
*This is a setting which automatically runs software on a DVD or memory stick. You can disable "auto-run" or "auto-play" on Windows through Settings, on macOS through System Preferences and on Linux through the settings app for your distribution. 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.*

| [Notes] |
| --- |

# Device Locking

A5.10. When a device requires a user to be present, do you set up 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.*

***This is a new requirement in Cyber Essentials. More information can be found in the 'Cyber Essentials Requirement for Infrastructure v3.0' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf***

| [Notes] |
|---|

A5.11. Which method do you use to unlock the devices and what brute force protection is in place?

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

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

| [Notes] |
|---|

# Security update management

**To protect your organisation, you should ensure that all your software is always up to date with the latest patches. If, on any of your in-scope devices, you are using an operating system which is no longer supported, (e.g., Microsoft Windows XP/Vista/2003 or macOS El Capitan, Ubuntu 17.10), and you are not being provided with updates from another reliable source, 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.**

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

*Older operating systems that are out of regular support include Windows XP/Vista/Server 2003, mac OS Mojave, iOS 12, iOS 13, Android 8, and Ubuntu Linux 17.10. This requirement includes the firmware on your Firewalls and Routers. 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.*

[Notes]

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

*All software used by an organisation must be supported by a supplier who provides regular security updates. Unsupported software must be removed from devices. This includes frameworks and plugins such as Java, Adobe Reader, and .NET.*

[Notes]

A6.2.1 Please list your Internet Browser/s.

*Please list all internet browsers you use so that the assessor can understand your setup and verify that they are in support. For example: Chrome Version 89; Safari Version 14.*

[Notes]

A6.2.2 Please list your Malware Protection.

*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; Windows Defender; Bitdefender Internet Security 2020.*

[Notes]

A6.2.3 Please list your Email Applications installed on end user devices and sever.

*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.*

[Notes]

A6.2.4 Please list all Office Applications that are used to create organisational data.

*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.*

[Notes]

A6.3. Is all software licensed in accordance with the publisher's recommendations?

*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.*

[Notes]

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

*You must install any such updates 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.*

[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.*

[Notes]

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

*It is not always possible to apply auto updates. Please indicate how any updates are applied when auto updates are not configured*

[Notes]

A6.5. Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Java, Adobe Reader and .Net.) installed within 14 days of release?
*You must install any such updates 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.*

[Notes]

A6.5.1 Are all updates applied for applications by enabling auto updates?
*Most devices have the option to enable auto updates. Auto updates should be 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?
*Please indicate how updates are applied when auto updates have not been configured.*

[Notes]

A6.6. Have you removed any software on your devices that is no longer supported and no longer receives updates 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, frameworks such as Java and Flash, and all application software.*

[Notes]

A6.7. Where unsupported software is in use, have those devices been moved to a segregated sub-set and internet access removed and how do you achieve this?
***This question is for information only. From January 2023 this question will require that all unsupported software has been moved to a segregated sub-set and internet access removed and will be marked for compliance.***

*Software that is not removed from devices when it becomes un-supported will need to be placed onto its own sub-set and prevented from inbound and outbound internet access.*

*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.*

[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.**

A7.1. Are 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.*

| [Notes] |
|---|

A7.2. Are all user and administrative accounts accessed by entering a unique username and password?

*You must ensure that no devices can be accessed without entering a username and password.*

***Accounts must not be shared.***

| [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.*

| [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.*

| [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 confirm how this is recorded?
*You must have a formal, written-down 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.*

[Notes]

A7.6. How do you ensure that administrator accounts are used only 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 through separate accounts.*

[Notes]

A7.7. How does the organisation prevent administrator accounts from being used to carry out everyday tasks like browsing the web or accessing email?
*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 and procedure as well as regular training for staff.*

[Notes]

A7.8. Do you formally track which users have administrator accounts in your organisation?
*You must track by means of list or formal record all people that have been granted administrator 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.*

| [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.

This requirement has been updated. More information can be found in the 'Cyber Essentials requirement for Infrastructure v3.0' document. Link is referenced in question A1.11.

A7.10. Describe how you protect accounts from brute-force password guessing in your organisation?
*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 Access Control section in the 'Cyber Essentials Requirements for IT Infrastructure' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

[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 new section about Password-based authentication in the 'Cyber Essentials Requirements for IT Infrastructure' document. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

[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.*
*https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf*

[Notes]

A7.13. Do you have a documented password policy that includes 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 an account has been compromised.*

[Notes]

A7.14. Have you enabled Multi-Factor Authentication (MFA) on all of your cloud services?
*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 for users and administrators. For more information see the NCSC's guidance on MFA.*
*https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services*

[Notes]

A7.15. If no, is this because MFA is not available for some of your cloud services? List the cloud services that do not allow multi-factor authentication.
*It is required to provide a list of cloud services that are in use that do not provide 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.*

[Notes]

A7.17. Has MFA been applied to **all** users of your cloud services?
***This question is currently for information only. From January 2023 this question will require that all user accounts are protected by MFA on cloud services and marked for compliance.***

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

[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 both malware signatures and heuristic 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.

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 to an approved set (i.e., using an App Store and a list of approved applications) and/or:

C - application sandboxing (i.e., by using a virtual machine)?

*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.*

| [Notes] |
|---|

A8.2. If Option A: Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access?

*This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-virus software. You can use any commonly used anti-virus 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.*

| [Notes] |
|---|

A8.3. If Option A: 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-virus software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.*

| [Notes] |
|---|

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

*By default, most mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.*

| [Notes] |
|---|

A8.5. If Option B: 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 document 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.*

| [Notes] |
|---|

A8.6. If Option C: Where you use application sandboxing, do you ensure that applications within the sandbox are unable to access data stores, sensitive peripherals, and your local network? Describe how you achieve this.

*If you are using a virtual machine to sandbox applications, you can usually set these settings within the configuration options of the virtual machine software.*

| [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.