Cybiss
Information Security

Cyber Essentials
Self-Assessment Preparation Booklet

Version 11

January 2019

Introduction

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

Cyber Essentials

Cyber Essentials is a government-backed scheme focusing on the 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.

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.

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 name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity.

[Notes]

A1.2. 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.

[Notes]

A1.3. 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]

A1.4. 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]

A1.5. 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]

A1.6. What is the size of your organisation?

Based on the EU definitions of Micro (<10 employees, < €2m turnover), Small (<50 employees, < €10m turnover) , Medium (<250 employees, < €50m turnover) or Large.

[Notes]

A1.7. How many staff are home workers?

Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when travelling.

[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 business information 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".

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 company excluding development network").

[Notes]

A2.5. 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]

A2.6. Please list the quantities of laptops, computers and servers within the scope of this assessment. You must include the model and operating systems versions for all devices.

All laptops, computers, and servers that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information.

[Notes]

A2.7. 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 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. You do not need to provide serial numbers, mac addresses or other technical information.

[Notes]

A2.8. 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). You do not need to provide IP addresses or other technical information.

[Notes]

A2.9. Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers).

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.

[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]

Office Firewalls and Internet Gateways

Firewall is the generic name for software or hardware which provides technical protection between your systems and the outside world. There will be a firewall within your internet router. Common internet routers are BT Home Hub, Virgin Media Hub or Sky Hub.

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

Questions in this section apply to: Hardware Firewall devices, Routers, Computers and Laptops only.

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

You must have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network.

[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? How do you achieve this?

The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub) you can change the default password by logging into the web interface for the device (often located at 192.168.1.1 or 192.168.1.254).

[Notes]

A4.3. Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess?

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]

A4.4. Do you change the password when you believe it may have been compromised? How do you achieve this?

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]

A4.5. Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case?

At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a VPN server, a mail 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. The business case should be documented and recorded.

[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? Describe the 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).

[Notes]

A4.7. Have you configured your internet routers or hardware firewall devices 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 internet routers or hardware 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 two-factor authentication or by only allowing trusted IP addresses to access the settings? List 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 computers and laptops?

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". You can also use the firewall that may be provided by your anti-virus software.

[Notes]

A4.12. If no, is this because software firewalls are not commonly available 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, Computers, Laptops, Tablets and Mobile Phones.

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, computers, servers, tablets and mobile phones? 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.

[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 no 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 laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?

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]

5.4. Do all your users and administrators use passwords of at least 8 characters?

The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.

[Notes]

A5.5. Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet?

Your business might run software that allows people outside the company on the internet to access information within your business via an external service. This could be a VPN server, a mail server, or an internet application that you provide to your customers as a product. In all cases these applications provide information is confidential to your business and your customers and that you would not want to be publicly accessible. This question does not apply to cloud services such as Google Drive, Office365 or Dropbox. If you only use such services and do not run your own service you should answer no to this question.

[Notes]

A5.6. If yes, do you ensure all users of these services use a password of at least 8 characters and that your systems do not restrict the length of the password?

The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.

[Notes]

A5.7. If yes, do you ensure that you change passwords if you believe that 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]

A5.8. If yes, are your systems set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?

The external service that you provide must be set to slow down to 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]

A5.9. If yes, do you have a password policy that guides all your users?

The password policy must include: guidance on how to choose non-guessable passwords, 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]

A5.10. 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]

Software Patching

To protect your organisation, you should ensure that 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, Computers, Laptops, Tablets, Mobile Phones, Routers and Firewalls.

A6.1. Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?

Please list the operating systems you use so that the assessor can understand your setup and verify that all your operating systems are still in support. Older operating systems that are out of support include Windows XP/Vista/2003, mac OS El Capitan and Ubuntu Linux 17.10

[Notes]

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

Please summarise the applications you use so the assessor can understand your setup and confirm that all applications are supported. This includes frameworks and plugins such as Java, Flash, Adobe Reader and .NET

[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.

[Notes]

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

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. Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this.

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]

A6.6. Have you removed any applications on your devices that are no longer supported and no longer receive regular fixes for security problems?

You must remove older applications from your devices when they are no longer supported by the manufacturer. Such applications might include older versions of web browsers, frameworks such as Java and Flash, and all application software.

[Notes]

User Accounts

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, Computers, Laptops, Tablets and Mobile Phones.

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. Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?

You must ensure that no devices can be accessed without entering a username and password. Users cannot share accounts.

[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 access privileges to systems and data.

[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, Computers, Laptops, Tablets and Mobile Phones.

A7.5. Do you have a formal process for giving someone access to systems at an "administrator" level? Describe the process.

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 staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?

You must ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware.

[Notes]

A7.7. How do you ensure that administrator accounts are not used for accessing email or web browsing?

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. 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]

A7.10. Have you enabled two-factor authentication for access to all administrative accounts?

If your systems supports two factor authentication (where you receive a text message, a one-time code, use a finger-print reader or facial recognition in addition to a password), then you must enable this for administrator accounts.

[Notes]

A7.11. If no, is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication.

You are not required to purchase any additional hardware or install additional software in order to meet this requirement. Most standard laptops do not have two-factor authentication available. If your systems do not have two-factor authentication available answer yes to this question.

[Notes]

Malware protection

Malware (such as computer viruses) is generally used to steal or damage information. Malware are 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 focused 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 are 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: Computers, Laptops, Tablets and Mobile Phones.

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

A - having anti-malware software installed,

B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) 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, process 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]