Cyber Essentials
Self-Assessment Preparation Booklet

SOUTHERN IT
NETWORKS

Version 10.8

May 2018

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 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

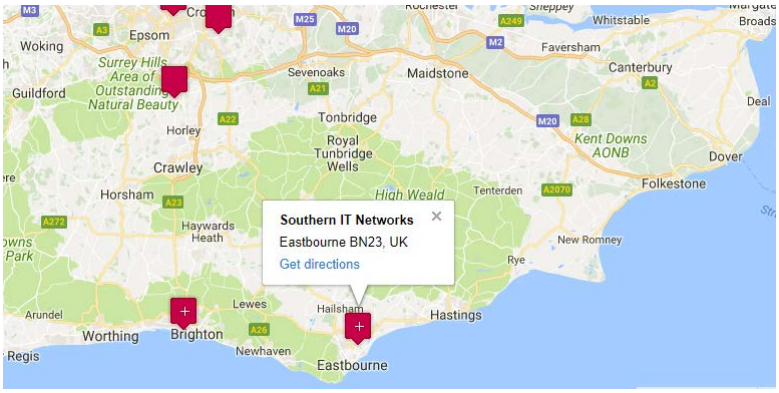
The booklet is intended to help you to understand the questions and take notes on the current setup in your organisation. In order to complete assessment, you must enter your answers via our online assessment platform.

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.

About Southern IT Networks

We are a Certification Body, trained approved and licensed by IASME, one of 5 Certification authorities approved by the NCSC (part of GCHQ). That means we can certify your business to the Cyber Essesntials, Cyber Essentials Plus and IASME Governance standards. We are one of only a handful of IASME certification bodies in the whole region and offer everything from full Online self certifications to fully managing the whole process for you.



Need help?

If you need help with understanding the questions, get in contact with Southern IT on +44 (0)1323 287828 or email CyberEssentials@SouthernIT.com

Your Company

Please tell us a little about how your company is set up

1. What is your organisation's name (for companies: as registered with Companies House)?

[Notes]

2. What is your organisation's registration number (if you have one)?

[Notes]

3. What is your organisation's address (for companies: as registered with Companies House)?

[Notes]

4. What is your main business?

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]

5. What is your website address?

[Notes]

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]

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

Please briefly 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".

8. 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.

[Notes]

9. If it is not the whole organisation, then what scope description would you like to appear on your certificate and website?

[Notes]

10. Please describe the geographical locations of your business which are in the scope of this assessment.

[Notes]

11. Please list all equipment which is included in the scope of this assessment (please include details of laptops, computers, servers, mobile phones and tablets).

All laptops, computers, servers and mobile devices that can access business data and have access to the internet must be included in the scope of the assessment.

[Notes]

12. Please provide details of the networks that will be in the scope for this assessment (such as office network, home offices and firewalls).

[Notes]

13. Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment?

[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

14. Do you have firewalls at the boundaries between your organisations internal networks and the internet?

You should 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. Remember most internet-routers contain a firewall.

[Notes]

15. 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?

[Notes]

16. 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 not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345".

[Notes]

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

[Notes]

18. 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 server or a video conferencing unit). 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".

[Notes]

19. 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.

[Notes]

20. 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]

21. 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]

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

[Notes]

23. 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.

[Notes]

24. Do you have software firewalls enabled on all of your computers and laptops?

You can check this setting on Mac laptops in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings or Control Panel and searching for "windows firewall".

[Notes]

25. If no, is this because software firewalls are not commonly available for the operating system you are using? Please list the operating systems.

[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 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 operating systems and applications running on: Servers, Computers, Laptops, Tablets and Mobile Phones.

26. 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. This includes applications, system utilities and network services.

[Notes]

27. 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?

[Notes]

28. 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?

[Notes]

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

A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.

[Notes]

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

[Notes]

31. 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?

[Notes]

32. If yes, do you ensure that you change passwords if you believe that they have been compromised?

[Notes]

33. 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?

[Notes]

34. 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] ?

35. 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" through control panel / system preferences.

[Notes]

Software Patching

To protect your organisation, you should ensure that your software is always up-to-date with the latest updates or "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 or mac OS Mountain Lion, 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.

36. Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems? Please list any operating systems that are not supported.

[Notes]

37. Are all applications on your devices supported by a supplier that produces regular fixes for any security problems? Please list any applications that are note supported.

[Notes]

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

[Notes]

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

[Notes]

40. 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.

[Notes]

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

[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.

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

[Notes]

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

[Notes]

44. 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]

45. 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.

[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 day-to-day basis in a privileged "administrator" mode.

Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones.

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

[Notes]

47. How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?

[Notes]

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

[Notes]

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

[Notes]

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

[Notes]

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

[Notes]

52. 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.

[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 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 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.

53. 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 (ie using an App Store or application whitelisting) or

    C - application sandboxing (ie by using a virtual machine)?

[Notes]

54. 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.

[Notes]

55. 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?

[Notes]

56. 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 do not allow you to install unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.

[Notes]

57. 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?

[Notes]

58. 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]

Insurance

All organisations with a head office domiciled in the UK that have the whole company in scope and a turnover of < £20m get automatic cyber insurance if they achieve Cyber Essentials certification. The cost of this is included in the assessment package 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.

59. Is your head office domiciled in the UK and is your gross annual turnover less than £20m?

The answer to this question is just for information and, if you are eligible for the insurance and opt in, will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

If you have answered "yes" to the last question, then your company is eligible for the included cyber insurance if you gain certification. The cost of the insurance is included in the cost of the assessment

60. Do you want to accept this cyber insurance?

The answer to this question is just for information and, if you are eligible for the insurance and opt in, will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

61. What is your total gross revenue?

You only need to answer this question if you are taking the insurance. The answer to this question is just for information and will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

62. 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 is just for information and will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

63. 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 is just for information and will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

64. 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]

Achieving compliance with the Cyber Essentials profile or the IASME governance standard indicates that your organisation has taken the steps set out in the HMG Cyber Essentials Scheme documents or the broader IASME Governance standard. It does not amount to an assurance that the organisation is free from cyber vulnerabilities and neither IASME Consortium Limited (as Accreditation Body) 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.

A "pass" under the GDPR assessment does not mean that you are assessed as being legally compliant. It indicates only that your organisation is starting on the pathway to compliance and is committed to ensuring 'privacy by design'.

You should ensure that your organisation obtains specialist legal advice on the GDPR as on any other data protection issue. This GDPR assessment is not legal advice and must not be relied upon as such and IASME accepts no liability for loss or damage suffered as a result of reliance on views expressed here.

The full extent of the GDPR regime and its application post Brexit (for example) is not yet fully known but the assessment addresses what we consider to be key elements and to help organisations demonstrate progress towards meeting the policy objectives that underpins the GDPR.

If you are awarded a certificate you will also be sent a badge to use in correspondence and publicity. You must accept the conditions of use.