Cyber Essentials Questionnaire Guidance

Introduction

This document has been produced to help companies write a response to each of the questions and therefore provide a good commentary for the controls in use.

Please note that it is just a guide to help you understand what goes through an assessors mind when reading through responses.

It is possible to achieve certification without following the guidance prompts – however, this may result in more follow up calls from the Certification Body.

You must answer each of the 34 questions in the questionnaire which can be downloaded from http://www.indelibledata.co.uk/cyberessentials/

Organisation Identification

Please provide details as follows:

Organisation Name (legal entity):	
Sector:	
Parent Organisation name (if any):	
Size of organisation (Micro/SME/Large etc) No of employees	
Point of Contact name:	
Job Title:	
Email address:	
Telephone Number:	
Certifying Body (CB):	
CB Reference number:	

Business Scope

Please identify the scope of the system(s) to be assessed under this questionnaire, including locations, network boundaries, management and ownership. Where possible, include IP addresses and/or ranges.

A system name should be provided that uniquely identifies the systems to be assessed, and which will be used on any certificate awarded. (Note: it is not permissible to provide the company name, unless all systems within the organisation are to be assessed):

How many sites are in scope?
How are they connected?
Have out-of-scope areas been sufficiently segregated (NAT / Firewall)?

What Cloud Services are used (Dropbox, Office 365, Google Drive)

- Please provide a URL (or send supplemental documentation) that shows each cloud provider's security processes and certifications

This document has been prepared with the assistance of the IASME Consortium Ltd and CREST (GB) Ltd, and is derived from work carried out by those organisations under contract to HMG (BIS, CESG, Cabinet Office) during the development of the Cyber Essentials Scheme

Boundary Firewalls and Internet Gateways

	Question	Answer	Comment
1	Have you installed Firewalls or similar devices at the boundaries of the networks in the Scope?	Always Mostly Sometimes Rarely Never	Make of Firewalls? Who administers them? Example: Our Head office is protected by a Cisco SA 500 This was installed and is maintained by our outsourced IT company XX Solutions.
2	Have the default usernames/passwords on all boundary firewalls (or similar devices) been changed to a strong password	Always Mostly Sometimes Rarely Never	When was this done and who by (which department or provider?) What are the complexity rules of passwords? Example: The outsourced IT company have declared that they changed the password to one that requires 15 characters – mixture of upper and lower case, special char and a number.
3	Have all open ports and services on each firewall (or similar device) been subject to justification and approval by an appropriately qualified and authorised business representative, and has this approval been properly documented?	Always Mostly Sometimes Rarely Never	What is the approval process? Who administers this? Example: The Operations Manager issues a request ticket to the IT company stating the reason for the port to be open after considering security implications. The IT company then arrange a suitable time to perform the operation
4	Have all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec) been disabled or blocked by default at the boundary firewalls?	Always Mostly Sometimes Rarely Never	How do you know this to be the case? Who (role) did this and when was it last checked?

	Question	Answer	Comment
5	Confirm that there is a corporate policy requiring all firewall rules that are no longer required to be removed or disabled in a timely manner, and that this policy has been adhered to (meaning that there are currently no open ports or services that are not essential for the business)?	Policy exists and has been implemented Policy exists but has not been implemented Policy does not exist	What is the name of the corporate policy document? When was the last check performed to verify that the only ports open that are those essential for business? Who signs this off (name / role)?
6	Confirm that any remote administrative interface has been disabled on all firewall (or similar) devices?	Always Mostly Sometimes Rarely Never	 Checked by? When? If the firewall ever configured remotely by anyone (for example by IT Support) and if so how is this done? If the remote admin interface must be enabled, what other compensating controls are used?
7	Confirm that where there is no requirement for a system to have Internet access, a Default Deny policy is in effect and that it has been applied correctly, preventing the system from making connections to the Internet	Always Mostly Sometimes Rarely Never	 Do you have any machines that require this (i.e. you are keeping out of scope?) Does anyone browse the web on a server?

Please provide any additional evidence to support your assertions above:

Secure Configuration

	Question	Answer	Comment
8	Have all unnecessary or default user accounts been deleted or disabled	Yes No	 How do you know this? Whose role is it to check this? What is the process to ensure this is done?
9	Confirm that all accounts have passwords, and that any default passwords have been changed to strong passwords?	Always Mostly Sometimes Rarely Never	How was this achieved? Are technical controls in place to enforce complex passwords or is it paper based policy?
10	Has all unnecessary software, including OS utilities, services and applications, been removed or disabled	Always Mostly Sometimes Rarely Never	Whose role is it to commission a machine and how do they ensure that only approved services and applications have been installed and enabled? Is it part of policy to remove all unnecessary “bundled” software?
11	Has the Auto Run (or similar service) been disabled for all media types and network file shares?	Always Mostly Sometimes Rarely Never	How did you disable this (a screen shot may be useful)?
12	Has a host based firewall been installed on all desktop PCs or laptops, and is this configured to block unapproved connections by default?	Installed and configured Installed, but not configured Not installed	How do you know this (A screen grab to show this would be useful)?

13	Confirm that a standard build image is used to configure new workstations and that this image includes the policies and controls and software required to protect the workstation, and that the image is kept up to date with corporate policies?	Yes No	Who created the image (dept / role) and whose responsibility is it to keep it up to date? If a build image is not used – are build instructions or build best practice guidelines followed? If so, what are they?
14	Confirm that you have a backup policy in place, and that backups are regularly taken to protect against threats such as ransomware?	Yes No	Describe the backup process (online / Disk / Tape etc) and what makes you confident that malware that can encrypt everything the user can access will not affect the backups?
15	Confirm that security and event logs are maintained on servers, workstations and laptops?	Yes No	What logs are enabled?

Please provide any additional evidence to support your assertions above:

Access Control

	Question	Answer	Comment
16	Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals?	Yes No	Mention the New starters procedure if you have one. Describe the following process: • Requested by: • Approved by: • User added by:
17	Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?	Yes No	Have you identified any users that share login accounts – how are these managed?
18	Are accounts removed or disabled when no longer required?	Yes No	Mention the Leavers procedure if you have one. When did you last check that only valid users are on the system? Are regular checks done to ensure out of date accounts have been identified and removed?
19	Are elevated or special access privileges, such as system administrator accounts, restricted to a limited number of authorised individuals?	Yes No	What is the role of these individuals?
20	Are special access privileges documented and reviewed regularly (e.g. quarterly)?	Yes No	When did you last review the special access privileges? How are these documented (spreadsheet / database etc)

21	Are all administrative accounts only permitted to perform administrator activity, with no Internet or external email permissions?	Yes No	Domain and Local Computer Admins are included in this – what controls are in place to prevent this internet and email access for admins?
22	Does your password policy enforce changing administrator passwords at least every 60 days to a complex password?	Yes No	 How is this enforced? Would you like to justify more days? Use of password keepers?

Please provide any additional evidence to support your assertions above:

Malware Protection

	Question	Answer	Comment
23	Please confirm that malware protection software has been installed on at least all computers with an ability to connect outside of the network in Scope	Always Mostly Sometimes Rarely Never	What Malware protection software is used? How is it deployed?
24	Does corporate policy require all malware protection software to have all engine updates applied, and is this applied rigorously?	Yes No	This should be within 90 days.
25	Have all malware signature files been kept up to date (through automatic updates or through centrally managed deployment)?	Yes No	Are samples done? How do you know each machine is up to date?
26	Has malware protection software been configured for on-access scanning, and does this include downloading or opening files, opening folders on removable or remote storage, and web page scanning?	Yes No	Can users change this setting?
27	Has malware protection software been configured to run regular (at least daily) scans?	Yes No	Describe the scan regime – Full scan / quick scan / etc
28	Apart from Anti Virus Software, are commonly accessed executables protected from being attacked by malicious files?	Always Mostly Sometimes Rarely Never	How is this achieved? What mechanisms are in place to ensure that if a user clicks on a malicious link, the executable file does not execute?
29	Are users prevented from accessing known malicious web sites by your malware protection software through a blacklisting function?	Yes No	Does the AV do this or have you subscribed to a third party DNS service that filters such sites (name it)?

Please provide any additional evidence to support your assertions above:

Patch Management

	Question	Answer	Comment
30	Is all software installed on computers and network devices in the Scope licensed and supported?	Always Mostly Sometimes Rarely Never	If any software / OS is out of support, then how have you ensured that this is out of scope?
31	Are all Operating System security patches applied within 14 days of release?	Always Mostly Sometimes Rarely Never	How do you ensure this – are patches centrally deployed or individual machines set to automatically update for example?
32	Are all Application software security patches applied within 14 days of release?	Always Mostly Sometimes Rarely Never	How do you ensure this – are patches centrally deployed or individual machines set to automatically update for example?
33	Is all legacy or unsupported software isolated, disabled or removed from devices within the Scope?	Yes No	What process is used to record software on devices?
34	Is a mobile working policy in force that requires mobile devices (including BYOD) to be kept up to date with vendor updates and app patches?	Yes No	Do non-company owned devices connect to the business network? Is there a “Guest” partition where they connect? What sort of work is done via mobile devices?

Please provide any additional evidence to support your assertions above:

Approval

This document has been prepared with the assistance of the IASME Consortium Ltd and CREST (GB) Ltd, and is derived from work carried out by those organisations under contract to HMG (BIS, CESG, Cabinet Office) during the development of the Cyber Essentials Scheme

It is a requirement of the Scheme that a Board level (or equivalent) of the organisation has approved the information given. Please provide evidence of such approval:

A Signature (scanned) or an email from the senior director's email account is sufficient in most cases.