Cyber Essentials Questionnaire

IMPORTANT:
This document provides the self-assessment questions for Cyber Essentials certification, but excludes additional guidance offered by IT Governance to provide assistance with the application process. Visit the IT Governance FAQs page if you would like more information about the process.

When applying for certification through IT Governance, you will be able to complete the questionnaire provided online.

This document cannot be accepted for certification purposes.

Cyber Essentials Questionnaire

Contents

IT Governance © 2016
All Rights Reserved.

Page 2

Version 1.4
08/04/16

Classification: Public

Security controls questionnaire

Boundary firewalls and Internet gateways

Question	Response options		Justification (optional)
1. Have one or more firewalls (or similar network device) been installed on the boundary of the organisation's internal network(s)?	☐	Yes	Click here to enter text.
	☐	No	
2. Has the default administrative password of the firewall (or equivalent network device) been changed to an alternative strong password?	☐	Yes	Click here to enter text.
	☐	No	
	☐	No firewall present	
3. Has each open connection (i.e. allowed ports and services) on the firewall been subject to approval by an authorised business representative and documented (including an explanation of business need)?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
	☐	No firewall present	
4. Have vulnerable services (e.g. Server Message Block (SMB), NetBIOS, Telnet, TFTP, RPC, rlogin, rsh or rexec) been disabled (blocked) by default and those that are allowed have a business justification?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
	☐	No firewall present	
5. Have firewall rules that are no longer required been removed or disabled?	☐	Yes	Click here to enter text.
	☐	No	
	☐	No firewall present	
6. Are firewall rules subject to regular review?	☐	Yes	Click here to enter text.
	☐	No	

IT Governance © 2016
All Rights Reserved.

Page 3

Version 1.3
19/01/16

Classification: Public

	☐ No firewall present	

Question	Response options	Justification (optional)
7. Have computers that do not need to connect to the Internet been prevented from initiating connections to the Internet (Default deny)?	☐ Yes ☐ No	Click here to enter text.
8. Has the administrative interface used to manage the boundary firewall been configured such that it is not accessible from the Internet?	☐ Yes ☐ No	Click here to enter text.

Not for official certification purposes

IT Governance © 2016
All Rights Reserved.

Page 4

Version 1.3
19/01/16

Classification: Public

Secure configuration

Question	Response options		Justification (optional)
9. Are unnecessary user accounts on internal workstations (or equivalent Active Directory Domain) (eg Guest, previous employees) removed or disabled?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
10. Have default passwords for any user accounts been changed to a suitably strong password?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
11. Are strong, complex passwords defined in policy and enforced technically for all users and administrators?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
12. Has the auto-run feature been disabled (to prevent software programs running automatically when removable storage media is connected to a computer or network folders are mounted)?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
13. Has unnecessary (frequently vendor bundled) software been removed or disabled and do systems only have software on them that is required to meet business requirements?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	

IT Governance © 2016
All Rights Reserved.

Page 5

Version 1.3
19/01/16

Classification: Public

Cyber Essentials Questionnaire

Question	Response options		Justification (optional)
14. Is all additional software added to workstations approved by IT or Management staff prior to installation and are standard users prevented from installing software?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
15. Has a personal firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
16. Are all user workstations built from a fully hardened base platform to ensure consistency and security across the estate?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
17. Are Active Directory (or equivalent directory services tools) controls used to centralise the management and deployment of hardening and lockdown policies?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
18. Are proxy servers used to provide controlled access to the Internet for relevant machines and users?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
19. Is an offline backup or file journaling policy and solution in place to provide protection against malware that encrypts user data files?	☐	Yes always	Click here to enter text.
	☐	No	

IT Governance © 2016
All Rights Reserved.

Page 6

Version 1.3
19/01/16

Classification: Public

Cyber Essentials Questionnaire

Question	Response options		Justification (optional)
20. Is there a corporate policy on log retention and the centralised storage and management of log information?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	No	
21. Are log files retained for operating systems on both servers and workstations?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
22. Are log files retained for relevant applications on both servers (including DHCP logs) and workstations for a period of at least three months?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
23. Are Internet access (for both web and mail) log files retained for a period of least three months?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
24. Are mobile devices and tablets managed centrally to provide remote wiping and locking in the event of loss or theft?	☐	Yes always	Click here to enter text.
	☐	For most devices	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
	☐	N/A	

IT Governance © 2016
All Rights Reserved.

Page 7

Version 1.3
19/01/16

Classification: Public

Question	Response options		Justification (optional)
25. Is a Mobile Device Management solution in place for hardening and controlling all mobile platforms in use within the organisation??	☐	Yes always	Click here to enter text.
	☐	For most devices	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
	☐	N/A	

IT Governance © 2016
All Rights Reserved.

Page 8

Version 1.3
19/01/16

Classification: Public

Access control

Question	Response options	Justification (optional)
26. Is user account creation subject to a full provisioning and approval process?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
27. Are system administrative access privileges restricted to a limited number of authorised individuals?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
28. Are user accounts assigned to specific individuals and are staff trained not to disclose their password to anyone?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
29. Are all administrative accounts (including service accounts) only used to perform legitimate administrative activities, with no access granted to external email or the Internet?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
30. Are system administrative accounts (including service accounts) configured to require regular password changes?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.

IT Governance © 2016
All Rights Reserved.

Page 9

Version 1.3
19/01/16

Classification: Public

Question	Response options		Justification (optional)
31. Where password changes are required for system administrative accounts (including service accounts), how often are changes required?	☐	Every 30 days	Click here to enter text.
	☐	Every 60 days	
	☐	Every 90 days	
	☐	Every 180 days	
	☐	N/a or longer/ Never	
32. Are users authenticated using suitably strong passwords, as a minimum, before being granted access to applications and computers?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
33. Are user accounts removed or disabled when no longer required (e.g. when an individual changes role or leaves the organisation) or after a predefined period of inactivity (e.g. 3 months)?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
34. Are data shares (shared drives) configured to provide access strictly linked to job function in order to maintain the security of information held within sensitive business functions such as HR and Finance?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	

IT Governance © 2016
All Rights Reserved.

Page 10

Version 1.3
19/01/16

Classification: Public

Malware protection

Question	Response options	Justification (optional)
35. Has anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
36. Has anti-virus or malware protection software (including program/engine code and malware signature files) been kept up-to-date (either by configuring it to update automatically or through the use of centrally managed service)?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
37. Has anti-virus or malware protection software been configured to scan files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages when accessed (via a web browser)?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
38. Has malware protection software been configured to perform regular periodic scans (eg daily)?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.

IT Governance © 2016
All Rights Reserved.

Page 11

Version 1.3
19/01/16

Classification: Public

Question	Response options		Justification (optional)
39. Are users prevented from executing programs from areas of the disk to which they have write access?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	
40. Are users prevented from executing programs from areas of the disk to which temporary Internet files are downloaded?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	Never	

IT Governance © 2016
All Rights Reserved.

Page 12

Version 1.3
19/01/16

Classification: Public

Patch management

Question	Response options	Justification (optional)
41. Do you apply security patches to software running on computers and network devices?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
42. Has software running on computers that are connected to or capable of connecting to the Internet been licensed and supported (by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
43. Has out-date or older software been removed from computer and network devices that are connected to or capable of connecting to the Internet?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ Never	Click here to enter text.
44. Have all security patches for software running on computers and network devices that are connected to or capable of connecting to the Internet been installed within 14 days of release or automatically when they become available from vendors?	☐ Yes always ☐ In most cases ☐ Sometimes ☐ Rarely ☐ No updates available ☐ N/A	Click here to enter text.

IT Governance © 2016
All Rights Reserved.

Page 13

Version 1.3
19/01/16

Classification: Public

Question	Response options		Justification (optional)
45. Are all smart phones kept up to date with vendor updates and application updates?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	No updates available	
	☐	N/A	
46. Are all tablets kept up to date with vendor updates and application updates?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	No	
47. Do you perform regular vulnerability scans of your internal networks and workstations to identify possible problems and ensure they are addressed?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	No	
48. Do you perform regular vulnerability scans (annual or more frequent) of your external network to identify possible problems and ensure they are addressed?	☐	Yes always	Click here to enter text.
	☐	In most cases	
	☐	Sometimes	
	☐	Rarely	
	☐	No	

IT Governance © 2016
All Rights Reserved.

Page 14

Version 1.3
19/01/16

Classification: Public

Cyber Essentials Questionnaire

Cyber Essentials staff awareness

Question	Response options	Justification (optional)
49. Do all personnel involved with implementing the Cyber Essential Scheme have sufficient knowledge of the scheme to do so effectively?	☐ Yes ☐ Not sure ☐ No	Click here to enter text.
50. Could you identify which 3rd party services were in scope of the Cyber Essential Scheme requirements?	☐ Yes ☐ Not sure ☐ No	Click here to enter text.

IT Governance © 2016
All Rights Reserved.

Page 15

Version 1.3
19/01/16

Classification: Public