Cyber Essentials Scheme (CES)

Questionnaire Guide

CONTENTS

Scope of the Assessment 3
Assessment Format 3
Organisation details 3
Remote Vulnerability Scan (Stage 1 – Cyber Essentials) 4
Workstation Assessment (Stage 2 - Cyber Essentials PLUS only) 5
Cloud / Shared Services Assessment 6
Security Controls Questionnaire 7
Boundary firewalls and Internet Gateways 7
Secure configuration 8
Access control 10
Malware protection 12
Patch management 13

SCOPE OF THE ASSESSMENT

ASSESSMENT FORMAT

This document outlines the information 4ARMED requires in order to assess our clients for Cyber Essentials or Cyber Essentials PLUS.

Each of the following sections outlines the format of the self-assessment questionnaire which will be provided to customers upon agreement to proceed with 4ARMED. **Please do not attempt to complete this form, it is provided for guidance and preparation only.**

ORGANISATION DETAILS

The following information your organisation will be required.

TOPIC	RESPONSE	
Name of organisation		
Registered Address		
Company / Charity Number		
Sector		
Turnover		
Number of Employees		
Name of main contact		
Contact Job title		
Date of response		
Contact Email		
Contact Telephone		
CE Level Desired		*Cyber Essentials or Cyber Essentials Plus

REMOTE VULNERABILITY SCAN (STAGE 1 – CYBER ESSENTIALS)

Include the Internet presence of the entire organisation and may include multiple connections for some organisations.

Ensure all virtual hosts are captured where multiple websites are hosted on the same IP address.

Note: for shared platforms (eg Office 365, Google Mail/Docs etc.), these systems are not included within the scope of hands on testing but you must provide evidence of the chosen systems being covered by an existing approved accreditation (eg ISO27001)

IP Address (or range) v4 and v6 addresses	**Fully Qualified Domain Name (FQDN) *where appropriate**	**Nature & Description of System (eg, firewall, website, cms,)**	**System Ownership and Hosting (eg internal system, dedicated external hosted, dedicated cloud system, shared platform)**	**If out of scope, organisation should cite a reason why.**
162.159.245.171	*www.customer-company.org*	*Website*	*Internally Hosted - In Scope*	
162.159.245.171	*portal.customer-company.co.uk*	*Website*	*Internally Hosted - In Scope*	
162.159.245.172	*n/a*	*VPN Server*	*Internally Hosted - In Scope*	
216.58.208.78	*docs.google.com*	*Website*	*Shared Cloud Device - Out of Scope*	*Google claim ISO 27001 certification for this platform.*
191.234.6.156	*portal.office.com*	*Website*	*Shared Cloud Device - Out of Scope*	*Microsoft claim ISO 27001 certification for this platform.*
162.159.245.173	*dns.customer-company.org*	*DNS Server*	*Internally Hosted - In Scope*	
162.159.245.174	*mail.customer-company.co.uk*	*Mail Server*	*Internally Hosted - In Scope*	
162.159.245.0/24	*n/a*	*Docklands Data Centre Range*	*Internally Hosted - In Scope*	

WORKSTATION ASSESSMENT (STAGE 2 - CYBER ESSENTIALS PLUS ONLY)

Ensure a representative sample of each type of standard workstation or device build is included and that additional unique builds are included (e.g. all BYOD devices).

A representative workstation is a single instance of a common build, if no such common build exists, all workstations will require testing.

Description of the device (with unique ID such as serial number)	**Operating System**	**Username and password of a test user account representing the device's typical user.**	**Confirmation that the device and test account supplied have access to Email and Internet (web) access as would a typical user of the device.**	**Confirmation that admin access is available to device (for patch checks)**	**Test Location**
Standard Laptop Build Hostname: PC01234	*Windows 8.1*	*Username: ABC\bob Password: Password1*	*yes*	*yes*	*London office*
Standard Workstation Build Hostname: PC01235	*Windows 8.1*	*To be provided onsite*	*yes*	*yes*	*London office*
Standard iPhone Joe Bloggs' Phone	*iOS 8*	*To be provided onsite*	*yes*	*yes*	*London office*
Standard iPad Joe Bloggs' iPad	*iOS 8*	*To be provided onsite*	*yes*	*yes*	*London office*

Notes

1) *Personal devices used for business purposes (including laptops and tablets, known as Bring Your Own Devices or BYOD) are within the scope of the assessment.*
2) *Devices or workstations that do NOT have Email AND do NOT have Internet (web) access are outside the scope of the Cyber Essentials assessment.*

CLOUD / SHARED SERVICES ASSESSMENT

Please ensure the table below is completed for all shared services:

Description of the service (with unique customer ID where relevant)	**Supplier**	**Independent audit standards to which the suppliers has been previously assessed.**	**Evidence of certification provided to CB (website URLs, certificate numbers, name of independent audit bodies etc)**
Microsoft Office 365	Microsoft	ISO27001	Office 365 is certified to ISO 27001 as described here – http://office.microsoft.com/en-gb/business/office-365-trust-center-cloud-computing-security-FX103030390.aspx http://office.microsoft.com/en-gb/business/office-365-security-and-privacy-verified-by-a-third-party-FX103089231.aspx
Google Mail & Google Docs	Google	ISO 27001 SSAE 16 / ISAE 3402 audited Safe Harbour and FISM	Google Mail / Docs is certified as described here https://support.google.com/a/answer/60762?hl=en http://www.computerworlduk.com/news/security/3360345/google-apps-receives-iso-27001-security-certification/

Notes

1) *This table should only be completed for shared services – dedicated platforms should be included within the technical testing*
2) *Note remote services such as email or document stores should be included in Cyber Essentials but remote desktop (VDI) solutions are also relevant for Cyber Essentials PLUS.*

SECURITY CONTROLS QUESTIONNAIRE

BOUNDARY FIREWALLS AND INTERNET GATEWAYS

QUESTION	RESPONSE OPTIONS
1. Have one or more firewalls (or similar network device) been installed on the boundary of the organisation's internal network(s)?	Yes No
2. Has the default administrative password of the firewall (or equivalent network device) been changed to an alternative strong password?	Yes 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 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 In most cases Sometimes Rarely Never No firewall present
5. Have firewall rules that are no longer required been removed or disabled?	Yes No No firewall present
6. Are firewall rules subject to regular review?	Yes No No firewall present
7. Have computers that do not need to connect to the Internet been prevented from initiating connections to the Internet (Default deny)?	Yes No
8. Has the administrative interface used to manage the boundary firewall been configured such that it is not accessible from the Internet?	Yes No

SECURE CONFIGURATION

QUESTION	RESPONSE OPTIONS
9. Are unnecessary user accounts on internal workstations (or equivalent Active Directory Domain) (eg Guest, previous employees) removed or disabled?	Yes always In most cases Sometimes Rarely Never
10. Have default passwords for any user accounts been changed to a suitably strong password?	Yes always In most cases Sometimes Rarely Never
11. Are strong, complex passwords defined in policy and enforced technically for all users and administrators?	Yes always 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 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 In most cases Sometimes Rarely Never
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 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 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 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 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 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 No
20. Is there a corporate policy on log retention and the centralised storage and management of log information?	Yes always In most cases No
21. Are log files retained for operating systems on both servers and workstations?	Yes always 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 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 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 For most devices Sometimes Rarely

	Never N/A
25. Is a Mobile Device Management solution in place for hardening and controlling all mobile platforms in use within the organisation?	Yes always For most devices Sometimes Rarely Never N/A

ACCESS CONTROL

QUESTION	RESPONSE OPTIONS
26. Is user account creation subject to a full provisioning and approval process?	Yes always In most cases Sometimes Rarely Never
27. Are system administrative access privileges restricted to a limited number of authorised individuals?	Yes always In most cases Sometimes Rarely Never
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
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
30. Are system administrative accounts (including service accounts) configured to require regular password changes?	Yes always In most cases Sometimes Rarely Never

31. Where password changes are required for system administrative accounts (including service accounts), how often are changes required?	Every 30 days 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 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 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 In most cases Sometimes Rarely Never

MALWARE PROTECTION

QUESTION	RESPONSE OPTIONS
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
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
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
38. Has malware protection software been configured to perform regular periodic scans (eg daily)?	Yes always In most cases Sometimes Rarely Never
39. Are users prevented from executing programs from areas of the disk to which they have write access?	Yes always 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 In most cases Sometimes Rarely Never

PATCH MANAGEMENT

QUESTION	RESPONSE OPTIONS
41. Do you apply security patches to software running on computers and network devices?	Yes always In most cases Sometimes Rarely Never
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
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
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 Never
45. Are all smart phones kept up to date with vendor updates and application updates?	Yes always 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 In most cases Sometimes Rarely No updates available N/A
47. Do you perform regular vulnerability scans of your internal networks and workstations to identify possible problems and ensure they are addressed?	Yes always 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 In most cases Sometimes Rarely No