



Cyber Essentials Scheme (CES)

Questionnaire

No liability is accepted for loss or damage from any cause whatsoever from the use of the document.
CREST retains the right to alter the document at any time.

Scope of the Assessment

Organisation details

Please ensure the following data is captured prior to commencing a Cyber Essentials project.

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

Technology in scope

Technology used by organisations can be diverse and range from smartphones, tablets and laptops to large scale infrastructure, as well as the use of externally hosted systems. This implementation profile covers only the critical technical controls required to protect an organisation's most exposed technology against the commonest forms of Internet-based cyber threats. Technical testing covers a range of external infrastructure and corporate devices including workstations and other devices. The majority of shared service components hosted by third parties are beyond the scope of this audit and information should be provided to prove they have existing certifications in place for the services they provide. Infrastructure as a Service (IaaS) where the organisation controls and manages the operating system is in scope. This evidence will need to be reviewed by the Cyber Essentials CB consultant as part of the review.

Remote Vulnerability Scan (Stage 1 – Cyber Essentials)

Include cloud services that are part of the organisation’s infrastructure, even if they are out of scope for the assessment. Please provide as much information as possible and include all relevant DNS names.

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.

Workstation Assessment (Stage 2 - Cyber Essentials PLUS only)

A representative workstation is a single instance of a common build, if no such common build exists, all workstations will require testing. Where there are a number of workstations of the same build then the following sample size must be assessed:

Sample Size Table	
No. of end points (of same build)	Test sample
1	1
2-5	2
6-19	3
20-60	4
61+	5

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

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)

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

Firewalls

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 difficult to guess 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? If no then: a. Does the administrative interface require second factor authentication or is access limited to a specific address?	Yes No + Yes to 8a 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 difficult to guess password?	Yes always In most cases Sometimes Rarely Never

Question	Response Options
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

Question	Response Options
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
26. Remote (Internet) access to commercially or personal sensitive data and critical information requires authentication.	Yes No

Access control

Question	Response Options
27. Is user account creation subject to a full provisioning and approval process?	Yes always In most cases Sometimes Rarely Never
28. Are system administrative access privileges restricted to a limited number of authorised individuals?	Yes always In most cases Sometimes Rarely Never
29. 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
30. 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

Question	Response Options
31. Are system administrative accounts (including service accounts) configured to lock out after a number of unsuccessful attempts?	3 Failures 6 Failures 10 Failures >10 Failures Never
32. Is there a password policy covering the following points: a. How to avoid choosing obvious passwords (such as those based on easily-discoverable information). b. Not to choose common passwords (use of technical means, using a password blacklist recommended). c. No password reuse. d. Where and how they may record passwords to store and retrieve them securely. e. If password management software is allowed, if so, which. f. Which passwords they really must memorise and not record anywhere.	All 6 items >4 items >2 items 1 item None
33. Are users authenticated using difficult to guess passwords, as a minimum, before being granted access to applications and computers?	Yes always In most cases Sometimes Rarely Never
34. 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
35. 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
36. Which of the following does the organisation mainly rely on for malware protection: a. Anti-virus or Malware protection (continue to Q 37-40) b. Application whitelisting (Continue to Q 41-43) c. Application Sandboxing (Continue to Q 44)	a. b. c.
37. 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
38. 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

Question	Response Options
39. 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
40. Has malware protection software been configured to perform regular periodic scans (eg daily)?	Yes always In most cases Sometimes Rarely Never
41. Are all applications which execute on devices approved by the business and restricted by code signing or other protection mechanisms	Yes always In most cases Sometimes Rarely Never
42. Does the organisation maintain a list of approved applications	Yes No
43. Are users prevented from installing any other applications?	Yes No
44. Is any unknown code limited to execute within a sandbox and cannot access other resources unless the user grants explicit permission.	Yes No

Patch management

Question	Response Options
45. Do you apply security patches to all software running on computers and network devices?	Yes always In most cases Sometimes Rarely Never
46. 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
47. 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
48. 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

Question	Response Options
49. 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
50. 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
51. 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
52. 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