Cyber Essentials PLUS Compliance Report

Microsoft

May 2018

Prepared By: Daniel Pollard

Email: daniel.pollard@nccgroup.trust

Telephone: 0161 209 5539

NCC Group PLC - Security Testing Audit and Compliance

XYZ Building
2 Hardman Boulevard
Spinningfields
Manchester, M3 3AQ

www.nccgroup.trust

Proprietary Information

The content of this document should be considered proprietary information and should not be disclosed outside of Microsoft without NDA.

Document Version Control	
Data Classification	Company Sensitive and Proprietary
Client Name	Microsoft
Proposal Reference	MSFT-220
Document Title	Cyber Essentials PLUS Compliance Report
Author	Daniel Pollard

Document History			
Issue No.	Date of Issue	Issued by	Change Description
0.1	29/05/2018	Daniel Pollard	Draft for NCC Group internal review only
0.2	29/05/2018	Tristan Hodgson	Internal QA
1.0	29/05/2018	Daniel Pollard	Release to Customer
2.0	29/05/2018	Daniel Pollard	Release to Customer
3.0	21/06/2018	Tristan Hodgson	Release to Customer
4.0	23/07/2018	Tristan Hodgson	Release to Customer

Document Distribution List	
Janne Uusilehto	Project Sponsor, Microsoft
Daniel Pollard	Service Delivery Lead - Cyber Essentials, NCC Group

Table of Contents

Cyber Essentials Compliance Statement

Overall Rating **PASS**

Company Assessed	Microsoft	**Primary Contact**	Janne Uusilehto
Number of Target Groups (See page 7) **Total (failed)**	2 (0)	**Number of Failed Key Controls (See page 6)**	0/5
Assessment Company	NCC Group	**Cyber Essentials Test Specification Version**	3.1
Assessment Start Date	23rd May 2018 – 29th May 2018	**CES Questionnaire Version**	3.0
Recommended Reassessment Date	28th May 2019	**Report Template Version**	2.0

Cyber Essentials PLUS Assessment Scope Summary

This certification was based on an assessment of the Cyber Essentials test cases applied to the following target groups:

- Microsoft Azure Workstation
- Microsoft External Scope

The organisation seeking certification also filled out the Cyber Essentials Scheme (CES) Questionnaire. In addition to the test cases above, the answers provided in the questionnaire were used as input to this assessment.

The term “Target Group” is used here to mean the groups of systems that were in scope for this security assessment. Note that Certification Bodies have rigid guidelines that describe what areas of the business must be in scope and what types of systems must be in scope.

Each of these target groups is defined in the Technical Summary section below.

Assessment Authorisation

Authorisation to test was provided by Janne Uusilehto of Microsoft.

Caveats

The test scope was determined by Microsoft with guidance from NCC Group. The questionnaire was completed by Microsoft. The systems provided for test were confirmed as being representative of those in use across the wider customer estate. NCC Group accepts no responsibility arising from the supply of non-representative systems for review during the onsite audit.

Questionnaire Sign-off

The questionnaire was certified as being accurate by:

Name	Chris Ransom
Position	Senior Service Engineer
Date of Signature	23rd May 2018
Signed copy seen by	Daniel Pollard
Signed copy seen on	23rd May 2018

Assessment Staff

Role	Name	Qualification
Assessor	Daniel Pollard	CRT-PEN
Quality Assurance	Tristan Hodgson	CRT-PEN

1. Key Control Compliance Summary

This section summarises the assessment results by Key Control, taking into account the results for all Target Groups, the results of the questionnaire and all other stages of the assessment.

The Five Key Controls correspond to the five basic technical elements listed on the National Cyber Security Centre (NCSC) website:

https://www.ncsc.gov.uk/information/requirements-it-infrastructure-cyber-essentials-scheme

Cyber Essentials Key Control	Overall Status
Boundary firewalls and Internet Gateways	**PASS**
Secure configuration	**ACTION POINT**
Access control	**PASS**
Malware protection	**PASS**
Patch management	**PASS**

More detail is provided on the reason for the overall status in the Assessment Result Summary section.

2. Target Group Compliance Summary

This section summarises the outcome of assessment by Target Group, taking into account the results of tests against each Target Group. The questionnaire results are not reflected in this section.

Target Group	Overall Status
Microsoft External Scope	ACTION POINT
Microsoft Azure Workstation	PASS

More detail is provided on the reason for the overall status in the Assessment Result Summary section.

The Target Groups are defined in the Technical Summary section.

3. Assessment Result Summary

The subsections below mirror the stages of the Cyber Essentials assessment.

Within each subsection is a summary of the status for each Target Group against each of the 5 Cyber Essentials Key Controls. Note that some stages of the assessment test all 5 Key Controls, but others test only some of the Key Controls.

Stage 1: Cyber Essentials Scheme (CES) Questionnaire

The answers in the returned questionnaire were scored objectively using prescribed method that this identical across all providers under the CREST Accreditation Body. The table below summarises whether the threshold for compliance was achieved for each of the 5 Cyber Essentials Key Controls.

Cyber Essentials Key Control	Overall Status
Boundary firewalls and Internet Gateways	**PASS**
Secure configuration	**PASS**
Access control	**PASS**
Malware protection	**PASS**
Patch management	**PASS**

For further details about the questionnaire, refer to the questionnaire response submitted to the Certification Body.

Stage 1, Test 1: Vulnerability Scan for Stated IP Range

This section details the results for each target group that was subject to Vulnerability Scanning. The Technical Summary later in the document defines each target group and states the types of testing performed for each.

The reason for the overall status is explained further in the Threat Profile Test Results section.

Microsoft External Scope

Cyber Essentials Key Control	Overall Status
Boundary Firewalls & Internet Gateways	**PASS**
Secure Configuration	**ACTION POINT**
Patch Management	**PASS**

Stage 2, Test 2: Inbound email binaries and payloads

This section details the results for each target group that was subject to email testing. The Technical Summary later in the document defines each target group and states the types of testing performed for each.

The reason for the overall status is explained further in the Threat Profile Test Results section.

Microsoft Azure Workstation

Cyber Essentials Key Control	Overall Status
Malware Protection	**PASS**
Secure configuration	**PASS**

Stage 2, Test 3: Web Site Page with URLs Linking to Binaries

This section details the results for each target group that was subject to browser testing. The Technical Summary later in the document defines each target group and states the types of testing performed for each.

The reason for the overall status is explained further in the Threat Profile Test Results section.

Microsoft Azure Workstation

Cyber Essentials Key Control	Overall Status
Boundary firewalls and Internet Gateways	**PASS**
Malware Protection	**PASS**
Secure configuration	**PASS**

Stage 2, Test 4: Authenticated Vulnerability Scan of Workstations

This section details the results for each target group that was subject to authenticated vulnerability testing. The Technical Summary later in the document defines each target group and states the types of testing performed for each.

The reason for the overall status is explained further in the Threat Profile Test Results section.

Microsoft Azure Workstation

Cyber Essentials Key Control	Overall Status
Secure configuration	**PASS**
Access control	**PASS**
Malware protection	**PASS**
Patch management	**PASS**

4. Technical Summary

Scope Details – Stage 1 – External Testing

The section defines each of the target groups in the Scope Summary section and details the types of testing that were carried out against each and from where testing was carried out.

Microsoft External Scope

This target group is defined as:

- <REDACTED>
- <REDACTED>
- <REDACTED>
- <REDACTED>

Testing was carried out over the Internet from the NCC Group offices in Manchester.

Scope Details – Stage 2 – End User Device Testing

End User Devices are taken to mean the complete range of electronic devices used by an individual to access their data. This phase of testing relates to only EUDs and does not include server systems unless in use for Remote User Desktop purpose. EUDs are classified for testing and reporting in to two main categories, workstations and mobile devices as defined below.

"Workstation" as used in this section should be understood to mean any device running a mainstream desktop operating system. Examples include Windows 7, 8, 8.1 and 10; Ubuntu, Debian, Red Hat Linux; and OSX. Other traits of desktop operating systems can help in their classification: The use of a super user account (Administrator/root) is common for administration. Microsoft Surface Pro devices are therefore treated as Workstations.

"Mobile Device" as used in this section should be understood to mean any device that runs a mobile OS. Examples include Android and Apple iOS. Other traits of mobile operating systems that distinguish them from desktop operating systems include: a super user account is not typically used for administration of the device; the device can be reset to factory defaults. Chrome Books are therefore treated as Mobile Devices.

Microsoft Azure Workstation

This target group is defined as:

- 1 x Sample Windows 10 Laptop (Host REDACTED was used for testing)

The types of testing performed were:

- Inbound email binaries and payloads
- Web Site Page with URLs Linking to Binaries
- A full Authenticated vulnerability scan of host

Testing was carried out onsite at the Microsoft office.

5. Threat Profile Test Results

This section follows the same structure as the Assessment Result Summary section. A subsection is included for each stage of testing. Within those subsections, the test results for each target group are reported.

Stage 1, Test 1 – Vulnerability scan for external IP Range

Microsoft External Scope

Cyber Essentials Key Control:	Boundary Firewalls & Internet Gateways	**PASS**
Action Points	1. None	

Cyber Essentials Key Control:	Secure Configuration	**ACTION POINT**
Action Points	1. Update the TLS/SSL Configuration to fix the issues identified.	

Cyber Essentials Key Control:	Patch Management	**PASS**
Action Points	1. None	

Stage 2, Test 2: Inbound email binaries and payloads

Microsoft Azure Workstation

Cyber Essentials Key Control:	Malware Protection	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Secure Configuration	**PASS**
Action Points:	1. None	

Stage 2, Test 3: Web Site Page with URLs Linking to Binaries

Microsoft Azure Workstation

Cyber Essentials Key Control:	Boundary firewalls and Internet Gateways	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Malware Protection	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Secure Configuration	**PASS**
Action Points:	1. None	

Stage 2, Test 4: Authenticated Vulnerability Scan of Host

Microsoft Azure Workstation

Cyber Essentials Key Control:	Secure configuration	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Access control	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Malware Protection	**PASS**
Action Points:	1. None	

Cyber Essentials Key Control:	Patch Management	**PASS**
Action Points:	1. None	

6. Target Vulnerabilities and Weakness Summary

The following table provides a summary of the vulnerability and weakness information detected during the Cyber Essentials assessment. Further vulnerability information may also be included in the Target Vulnerabilities and Weakness Summary.

Microsoft External Scope

Issue ID	IP Address	Port	Vulnerability Title	Key Control	Compliance Status
MS-914	<REDACTED>	443/tcp	Untrusted TLS/SSL server X.509 certificate	**Secure Configuration**	ACTION POINT
MS-1041	<REDACTED>	443/tcp	Untrusted TLS/SSL server X.509 certificate	**Secure Configuration**	ACTION POINT
MS-1091	<REDACTED>	443/tcp	Untrusted TLS/SSL server X.509 certificate	**Secure Configuration**	ACTION POINT
MS-1103	<REDACTED>	443/tcp	Untrusted TLS/SSL server X.509 certificate	**Secure Configuration**	ACTION POINT

Microsoft Azure Workstation

Issue ID	Hostname	Vulnerability Title	Severity	Compliance Status
No Issues Found				

Appendix 1 Detailed Findings and Remediation Advice

External Scan: Microsoft External Scope

Untrusted TLS/SSL server X.509 certificate		
CVSS3: 6.5	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	ACTION POINT
Issue ID	**IP Address**	**Port**
MS-914	<REDACTED>	443/tcp
MS-1041	<REDACTED>	443/tcp
MS-1091	<REDACTED>	443/tcp
MS-1103	<REDACTED>	443/tcp

Description

The server's TLS/SSL certificate is signed by a Certification Authority (CA) that is not well-known or trusted.

This could happen if: the chain/intermediate certificate is missing, expired or has been revoked; the server hostname does not match that configured in the certificate; the time/date is incorrect; or a self-signed certificate is being used.

Remediation Details

Ensure the common name (CN) reflects the name of the entity presenting the certificate (e.g., the hostname). If the certificate(s) or any of the chain certificate(s) have expired or been revoked, obtain a new certificate from your Certificate Authority (CA) by following their documentation.

Questionnaire Responses

Boundary Firewalls & Internet Gateways

Question	Response
Have one or more firewalls (or similar network devices) been installed on the boundary of the organisation's internal network(s)?	Yes
Has the default administrative password of the firewall (or equivalent network device) been changed to an alternative strong password?	Yes
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
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
Have firewall rules that are no longer required been removed or disabled?	Yes
Are firewall rules subject to regular review?	Yes
Have computers that do not need to connect to the Internet been prevented from initiating connections to the Internet (Default deny)?	Yes
Has the administrative interface used to manage the boundary firewall been configured such that it is not accessible from the Internet?	Yes

Secure Configuration

Question	Response
Are unnecessary user accounts on internal workstations (or equivalent Active Directory Domain) (eg Guest, previous employees) removed or disabled?	Yes always
Have default passwords for any user accounts been changed to a difficult to guess password?	Yes always
Are strong, complex passwords defined in policy and enforced technically for all users and administrators?	Yes always
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
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
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
Has a personal firewall (or equivalent) been enabled on desktop PCs and laptops, and configured to disable (block) unapproved connections by default?	Yes always
Are all user workstations built from a fully hardened base platform to ensure consistency and security across the estate?	Yes always
Are Active Directory (or equivalent directory services tools) controls used to centralise the management and deployment of hardening and lockdown policies?	Yes always
Are proxy servers used to provide controlled access to the Internet for relevant machines and users?	Yes always
Is an offline backup or file journaling policy and solution in place to provide protection against malware that encrypts user data files?	Yes always
Is there a corporate policy on log retention and the centralised storage and management of log information?	Yes always
Are log files retained for operating systems on both servers and workstations?	Yes always

Are log files retained for relevant applications on both servers (including DHCP logs) and workstations for a period of at least three months?	In most cases
Are Internet access (for both web and mail) log files retained for a period of least three months?	In most cases
Are mobile devices and tablets managed centrally to provide remote wiping and locking in the event of loss or theft?	Yes always
Is a Mobile Device Management solution in place for hardening and controlling all mobile platforms in use within the organisation?	Yes always
Does remote (Internet) access to commercially or personal sensitive data and critical information require authentication?	Yes

Access Control

Question	Response
Is user account creation subject to a full provisioning and approval process?	Yes always
Are system administrative access privileges restricted to a limited number of authorised individuals?	Yes always
Are user accounts assigned to specific individuals and are staff trained not to disclose their password to anyone?	Yes always
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
Are system administrative accounts (including service accounts) configured to lock out after a number of unsuccessful attempts?	Never
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. d. If password management software is allowed, if so, which. e. Which passwords they really must memorise and not record anywhere.	All 6 points
Are users authenticated using suitably strong passwords, as a minimum, before being granted access to applications and computers?	Yes always
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
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

Malware Protection

Question	Response
Which of the following does the organisation mainly rely on for malware protection?	Application whitelisting
Are all applications which execute on devices approved by the business and restricted by code signing or other protection mechanisms?	Yes always
Does the organisation maintain a list of approved applications?	Yes
Are users prevented from installing any other applications?	Yes