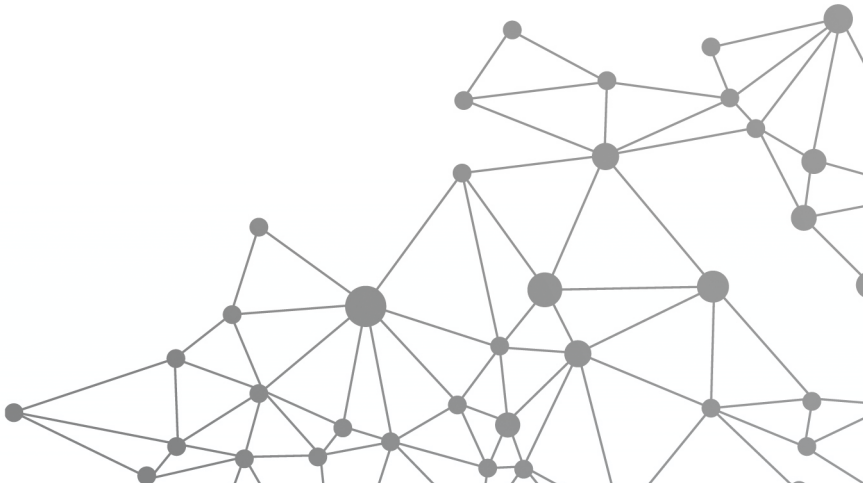
Cyber Essentials Compliance Report

NewRedo – UK Operations

20 February 2019



Version Control

Version	Date	Description	Released by
1.0	20/02/2019	Final Release	M. Wickenden

1 Contents

1 CONTENTS 3

CYBER ESSENTIALS COMPLIANCE STATEMENT 4

CYBER ESSENTIALS ASSESSMENT SCOPE SUMMARY 4
ASSESSMENT AUTHORISATION 4
CAVEATS 4
QUESTIONNAIRE SIGN-OFF 5
ASSESSMENT STAFF 5

2 KEY CONTROL COMPLIANCE SUMMARY 6

3 TARGET GROUP COMPLIANCE SUMMARY 7

4 ASSESSMENT RESULT SUMMARY 8

STAGE 1: CYBER ESSENTIALS SCHEME (CES) QUESTIONNAIRE 8
STAGE 1, TEST 1: VULNERABILITY SCAN FOR STATED IP RANGE 9

5 TECHNICAL SUMMARY 10

SCOPE DETAILS – STAGE 1 – EXTERNAL TESTING 10

6 THREAT PROFILE TEST RESULTS 11

STAGE 1, TEST #1 – VULNERABILITY SCAN FOR EXTERNAL IP RANGE 11

7 TARGET VULNERABILITIES AND WEAKNESS SUMMARY 12

OFFICE PERIMETER NETWORK 12

Cyber Essentials Compliance Statement

Overall Rating **PASS**

Company Assessed	NewRedo	**Primary Contact**	P. Luby
Number of Target Groups (See page 7) **Total (failed)**	1 (0)	**Number of Failed Key Controls (See page 6)**	0/5
Assessment Company	4ARMED	**Cyber Essentials Test Specification Version**	3.0
Assessment Dates	13 Dec 2019 – 18 Feb 2019	**CES Questionnaire Version**	3.2
Recommended Reassessment Date	19 February 2020	**Report Template Version**	6.0

CYBER ESSENTIALS ASSESSMENT SCOPE SUMMARY

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

- Office Perimeter Network

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

The assessment was authorised by P. Luby.

CAVEATS

No caveats apply.

QUESTIONNAIRE SIGN-OFF

The questionnaire was certified as being accurate by:

Name	**Phill Luby**
Position	**Director**
Date of Signature	**12th December 2018**
Signed copy seen by	**Marc Wickenden**
Signed copy seen on	**13th December 2018**

ASSESSMENT STAFF

Role	Name	Qualification
Assessor	**Marc Wickenden**	**CCT**

2 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 5 Key Controls correspond to the 5 basic technical elements listed on the 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	**PASS**
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.

3 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
Office Perimeter Network	**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.

4 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.

Office Perimeter Network

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

5 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.

Office Perimeter Network

NewRedo utilise a shared office environment and do not therefore have a dedicated connection which could be scanned. The external vulnerability scan was therefore descoped from the assessment work and personal firewalls on laptops provide the network perimeter.

6 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

Office Perimeter Network

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

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

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

7 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.

OFFICE PERIMETER NETWORK

Ref #	Vulnerability	CVSS2	Compliance Status
A1	N/A	N/A	N/A