Requirements for an Accreditation Body in the Cyber Essentials scheme

Version 3.1

November 2014

Version Control		
Date	**Version**	**Change**
15 Nov 14	3.1	Change DR5 to MR31, plus other general updates
22 Jul 14	3.0	Rewritten taking account of initial applications
18 Jun 14	2.0	Updated to reflect changes to contract on feedback from customers
6 Jun 14	1.0	First Issue of Document

Table of Contents

Introduction

This document sets out the Authority's requirements that are applicable to the Cyber Essentials Scheme Requirements

The Requirements have been derived from a number of sources, including ISO/IEC 27002:2005 Information technology – Security techniques – code of practice for information security management

Requirements are categorised as:

- Mandatory requirement (MR): identified by the use of the word 'shall'.
- Desirable requirement (DR): identified by the use of the word 'should'.
- Information statement (INFO): identified by the use of the word 'will'.

The Requirements given in this document provide the Authority with the assurance that an Accreditation Body will deliver the Cyber Essentials Scheme in an effective, efficient and competent manner, and that it will exercise sufficient control over the Certification Bodies under contract to it, and to ensure that whichever Certification Body carries out an evaluation, the result will be consistent. In order to achieve this, it is necessary for an Accreditation Body to provide evidence of the testing process and the competence of the Assessors and Certification Bodies.

Scope of Assessment for applications to be an Accreditation Body in the Cyber Essentials Scheme

The Requirements applicable to applications to the Cyber Essentials Scheme are set out below. These requirements shall be the basis for assessing applications to be an Accreditation Body under the terms of the Cyber Essentials Scheme, and the Authority may in due course publish an amended or reissued set of requirements for Cyber Essentials (which may be more extensive). Upon the Authority publishing Subsequent Requirements, any Accreditation Body (including the Contractor) operating under the Cyber Essentials Scheme will be expected to demonstrate its ability to meet those Subsequent Requirements within an agreed timescale.

Requirements

SERVICE MANAGEMENT	
MR1	The Accreditation Body shall have and duly administer a process for taking appropriate corrective action against Certification Bodies (including, without limitation, withdrawal or termination of any agreement to operate as a Certification Body under the Scheme) where it becomes aware (or is made aware) of any failure by a Certification Body to have and / or duly administer a process in accordance with the relevant subsequent Mandatory Requirements set out in this document.
INFO1	The Authority will be responsible for maintaining the Cyber Essentials Requirements, a Common Questionaire and a Common Testing Specification, and for making this available at no cost to the Accreditation Body, Certification Bodies and Customers.
INFO2	The Authority will endeavour to notify the Accreditation Body of significant changes to the Cyber Essentials Profile and Testing Specification.

CB ACCREDITATION SERVICE	
MR2	The Accreditation Body shall have and duly administer a process for receiving and recording applications to be a Certification Body
MR3	The Accreditation Body shall produce and make available to prospective Certification Bodies, a document detailing the Requirements of a Certification Body within the Accreditation Body's implementation of the scheme
MR4	The Accreditation Body shall hold Cyber Essentials certification at the level to which it delivers the scheme and shall provide proof to the Authority of such certification at its application and annually thereafter
MR5	The Accreditation Body shall have and duly administer a process for impartial assessment, using a defined set of criteria, of all applications to be a Certification Body
MR6	The Accreditation Body shall have and duly administer a process for informing applicants to be a Certification Body whether or not the application has been successful

SYSTEM EVALUATION SERVICE	
MR7	The Accreditation Body shall ensure that Certification Bodies hold Cyber Essentials certification at the level to which it delivers the scheme
MR8	The Accreditation Body shall produce a Guidance for Customers document to be disseminated by CBs to Service Users (i.e. the CB's Customers) detailing at least: • the System Evaluation processes at both Cyber Essentials and Cyber Essentials Plus • customer obligations through the process • branding guidelines

MR9	The Accreditation Body shall produce a common Questionnaire for customers requesting a Cyber Essentials audit, and make this available to Certification Bodies for their customers
MR10	The Accreditation Body shall produce guidance for Certification Bodies detailing the conduct of Level 1 (Cyber Essentials) auditing. This guidance shall include the Questionnaire to be completed by customers and pass or fail criteria to be used in assessing the customer Questionnaire.
MR11	Where it is intended to deliver Cyber Essentials Plus, the Accreditation Body shall either: • Adopt the CESG published Common Test Specification entirely and produce supporting tools and files as necessary • Produce a Test Specification for Certification Bodies detailing the testing process for Cyber Essentials Plus, that meets or exceeds the assurance provided by the CESG Common Test Specification. This Test Specification shall include pass or fail criteria for each test component, and will be subject to approval by the Authority..
MR12	The Accreditation Body shall have and duly administer a process for conducting regular audit of Certification Body results (at least annually), recording the results of such audit including any remedial actions required. Audit results shall be made available to the Authority on demand.
MR13	The Accreditation Body shall have and duly administer a process for ensuring that Certification Bodies have a process for conducting evaluations required by the Scheme (at either or both of Cyber Essentials and/or Cyber Essentials Plus) and in accordance with guidance documents or test specifications provided by the Accreditation Body; and that such process enables the Certification Body to satisfy itself that: • At Cyber Essentials, the response to a questionnaire provides sufficient evidence that the Controls required by the Scheme have been correctly implemented • At Cyber Essentials Plus (where applicable), appropriate testing has been conducted in accordance with an approved Testing Specification, and the results show that the Controls are effective
MR14	The Accreditation Body shall ensure that Certification Bodies have a process for recording and storing results of audit or testing evaluations
MR15	The Accreditation Body shall ensure that Certification Bodies have a process for awarding Accreditation Body endorsed certificates to customers whose evaluation has been successful or providing appropriate feedback where it was not
MR16	The Accreditation Body shall ensure that the Certification Bodies have a complaints and appeals process for customers, including an escalation process to raise complaints or appeals to the Accreditation Body
MR17	The Accreditation Body shall have and duly administer a complaints and appeals process able to handle complaints or appeals originating from customer (escalated) or Certification Body, including an escalation process to raise complaints or appeals to the Authority.
DR1	The Accreditation Body should satisfy itself that the Certification Body's solution will have the flexibility of evaluating information systems managed by Customers that include additional controls that are not specified in the Cyber Essentials profile
DR2	The Accreditation Body should ensure that Certification Bodies have a process to issue timely reminders to recertify to customers with previously certified systems

BRANDING	
MR18	The Accreditation Body shall design certificates for use by the Certification Bodies, with due regard for security and fraud prevention, and make these available to the Certification Bodies.
MR19	The Accreditation Body shall create and enforce a branding sub-licence agreement which will be used to sub-licence use of the certification mark graphic to Certification Bodies and onward to customers
MR20	The Accreditation Body shall ensure that certificates for issue comply with the Branding licence, sub-licence and guidelines, in particular that the licence incorporates the Certification Mark.
MR21	The Accreditation Body shall ensure that certificates are issued with a Date Of Issue clearly shown (with a statement that systems should be retested within 1 calendar year from the Date of Issue), and that they are issued with the name of the specific system tested or evaluated under the Cyber Essentials Scheme.
MR22	The Accreditation Body, on becoming, or being made aware of, the misuse of the certification mark graphic or any other Cyber Essentials mark: • by any of its contracted Certification Bodies or their customers, shall take prompt action and inform the Authority in a timely manner. • Where outside the Accreditation Body's implementation of the scheme, shall bring the misuse to the attention of the Authority in a timely manner
MR23	The Accreditation Body shall ensure that the certification mark graphic is used only to indicate a successfully certified information system.
MR24	The Accreditation Body shall ensure that the Certification Body is licensed to use the Cyber Essentials logo, not the certification mark graphic, to promote or otherwise advertise Cyber Essentials
INFO3	Customers will use the certification mark graphic only to promote certified information systems, rather than imply organisational certification.

ORGANISATIONAL REQUIREMENTS	
MR25	The Accreditation Body shall document a process detailing methods by which it shall ensure review and continual improvement, development and maintenance of its Cyber Essentials operation
MR26	The Accreditation Body shall ensure records relating to Management Information and Scheme performance (as described in the Scheme MI document and published on the Scheme Library web pages; as may be amended from time to time), are gathered and maintained in an industry recognised format
MR27	The Accreditation Body shall provide the Authority with a monthly report relating to Cyber Essentials MI, sent electronically in a format defined by the Authority
DR3	The Accreditation Body should inform the Authority of any disputes with Customers relating to security or confidentiality issues
DR4	The Accreditation Body should ensure that the Certification Body should seek to minimise the number of significant changes to their Customer fees and/or charging structure

INFO4	At Scheme review meetings the Accreditation Body will be expected to provide feedback on the Authority's Cyber Essentials Profile and Testing Specification.
INFO5	To support the development of Cyber Essentials the Authority will endeavour to share available information it has regarding Cyber Essentials certifications, the likely volume of future certification requests from Customers and/or related developments
INFO6	The Accreditation Body will request that the Certification Body will design its solution such that in the future all reporting and feedback activity can be completed via a direct input online portal service established by the Authority.
INFO7	The Accreditation Body will require that the Certification Body will design its solution such that in the future it can work with a single (possibly non-governmental) Service Owner

ASSESSORS	
MR28	The Accreditation Body shall create and maintain a code of practice for certification assessors and documentation detailing assessor competence criteria (see DR5).
MR29	The Accreditation Body shall review documentation relating to competence requirements and the code of practice for certification assessors at least annually.
MR30	The Accreditation Body shall have, and shall ensure that Certification Bodies have, a process for identifying and addressing conflicts of interest in the scheme business, howsoever arising.
MR31	The Accreditation Body shall ensure that minimum competence criteria for assessors: • For Cyber Essentials include relevant and current auditing and technical competencies and qualifications • For Cyber Essentials Plus are defined as holding a CESG Certified Professional certificate as a Penetration Tester (Practitioner) or equivalent, and are supervised by a CESG Certified Professional (Penetration Tester) (Senior) or equivalent.

SCHEME MARKETING	
Ref	Requirement
DR6	The Accreditation Body should publish details of Cyber Essentials and related promotional events on its website.
DR7	The Accreditation Body should share details of its forthcoming significant marketing and promotional activities with the Authority, particularly when being held at UK Government institutions.
INFO8	The Authority will make information on Cyber Essentials freely available on GOV.UK website.

SCHEME MARKETING	
Ref	Requirement
INFO9	The Accreditation Body will ensure that the Certification Body will be responsible for marketing its individual activities under Cyber Essentials, and the funding of such marketing.
INFO10	The Authority will endeavour to hold events related to Cyber Essentials and may discuss joint marketing opportunities prior to these events with the Accreditation Body and relevant Certification Bodies.
INFO11	The Authority will endeavour to provide reasonable assistance and support to the Accreditation Body's marketing and promotional activities, particularly when being held at UK Government institutions.