HM Government

CYBER ESSENTIALS

Cyber Essentials Scheme

Assurance Framework

January 2015

Contents

Introduction

The Cyber Essentials scheme has been developed by Government and industry to fulfil two functions. It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the 10 Steps to Cyber Security. And through the Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. We believe that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does is to define a focused set of controls which will provide cost-effective, basic cyber security for organisations of all sizes.

The Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, has been designed in consultation with SMEs to be light-touch and achievable at low cost. The two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It is important to recognise that certification only provides a snapshot of the cyber security practices of the firm at that time, while maintaining a robust cyber security stance requires additional measures such as a sound risk management approach, as well as on-going updates to the Cyber Essentials control themes, such as patching. But we believe this scheme offers the right balance between providing additional assurance of an organisation’s commitment to implementing cyber security to third parties, while retaining a simple and low cost mechanism for doing so.

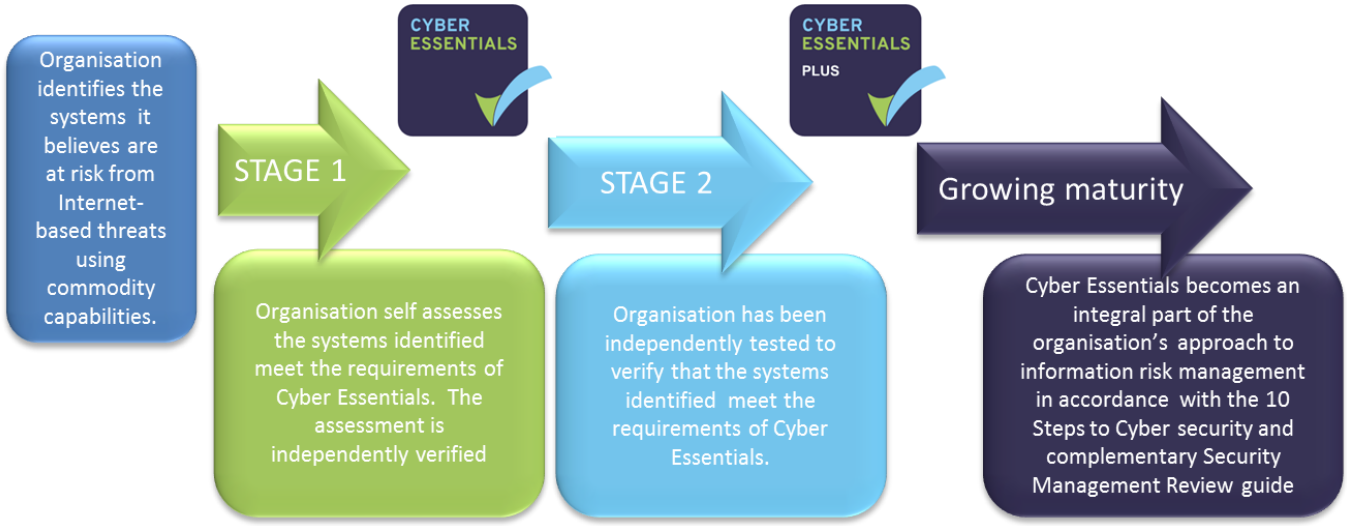
Change from June 2014 version

The only change from the previous version of this Assurance Framework is the removal of the option for an organisation to be both an Accreditation Body and a Certification Body.

Overview

The Assurance Framework provides organisations with a staged approach towards embedding mature and sustainable information risk management from common Internet based threats as well as the broader risks they might face. Each stage adds confidence and it is for organisations to decide which they choose based on their risk appetite, their customers' expectations and cost considerations.

The Framework supplements other information security certification arrangement s and covers the basic controls needed to defeat unsophisticated threats from the Internet. It defines two stages:



Stage Definitions

Stage 1 – Cyber Essentials: verified self-assessment

- Certification at this stage provides a basic level of confidence that the controls have been implemented correctly, and relies on the organisation having the skills to respond appropriately to the questionnaire.

- The scope must be declared at this stage. The scope should be defined in terms of network boundaries, location and management control.

- The organisation identifies the enterprise IT systems it believes are at risk from Internet based threat actors with low levels of technical capability and implements the Cyber Essentials requirements for basic technical cyber protection. Further guidance can be found on page 9.

- The organisation declares its compliance with the Cyber Essentials requirements so that it can be verified by a Certification Body.

- The declaration is signed by the Chief Executive Officer or equivalent endorsing its accuracy.

- The declaration is sent to a Certification Body for verification. If the Certification Body has sufficient confidence that the controls have been effectively implemented a certificate is awarded.

Stage 2 – Cyber Essentials Plus: independently tested

- Cyber Essentials is an integral part of Cyber Essentials Plus.

- This stage tests whether the controls implemented are sufficient to protect the organisation against Internet based threat actors with low levels of technical capability.

- The stage will be based on vulnerability testing of the system(s) in scope from inside and outside the system.

- The assessment can either directly test that individual controls have been implemented correctly or recreate various attack scenarios to determine whether they can achieve a compromise with widely available capabilities

Cyber Essentials Plus encompasses the same control themes as Cyber Essentials. Cyber Essentials Plus offers a higher level of assurance through the use of an independent testing regime.

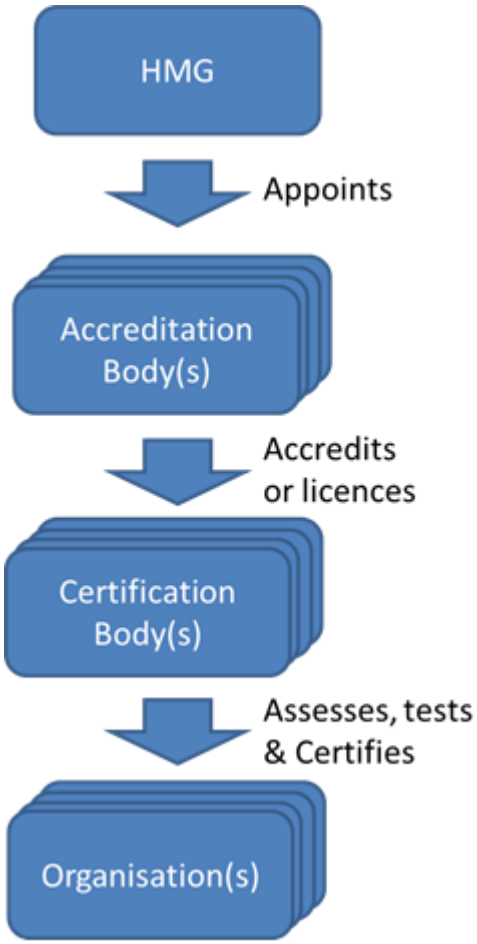
Certification at either Cyber Essentials or Cyber Essentials Plus should be seen as a snapshot of the organisation’s ability to mitigate the risks from the given Internet based threats at the time of assessment. It does not indicate how sustainable this will be.

Organisations will need to recertify once a year, or more frequently as necessary to meet specific procurement or customer requirements.

Implementation approach

Government has established a scalable framework of Accreditation and Certification Bodies[1]. HMG appoints Accreditation Bodies for Cyber Essentials and Cyber Essentials Plus, who in turn appoint Certification Bodies who can certify organisations that comply with Cyber Essentials requirements.

This approach allows scalability but also consistency across accreditation and certification bodies.



Role of Accreditation Bodies

Organisations may apply to Government to be appointed as an Accreditation Body (AB) for either Cyber Essentials or Cyber Essentials Plus or both. The role of an AB is to:

- Develop and own a certification process approved by HMG for assessing compliance with the applicable stage requirements.

[1] The Accreditation Bodies appointed under the Cyber Essentials Scheme are performing accreditation activities solely in relation to this particular UK scheme and are not performing accreditation services in relation to EU harmonised standards. The national accreditation body authorised to perform EU-harmonised accreditation services within the UK remains UKAS.

- Develop and own a certification process approved by HMG for assessing compliance with the applicable stage requirements. The certification process shall cover:
    - The tests to be undertaken.
    - The skills or qualifications required of the assessors and their supervisors.
    - The functionality required of any tools.
    - The minimum content of test reports.
    - The criteria for granting certification.
    - The content of certificates.
- Accredit (or license) companies as Certification Bodies who show they have the competence to implement the certification process.
- Ensure consistency of approach across their accredited companies, including adherence to any reporting standards.
- Set requirements for their Certification Bodies to protect client information shared with them.
- Arbitrate in disputes between Certification Bodies and their clients over Cyber Essentials certification results.
- Provide agreed management information to HM Government to enable adoption rates to be gauged.

For Cyber Essentials the certification process shall evidence that the organisation has:

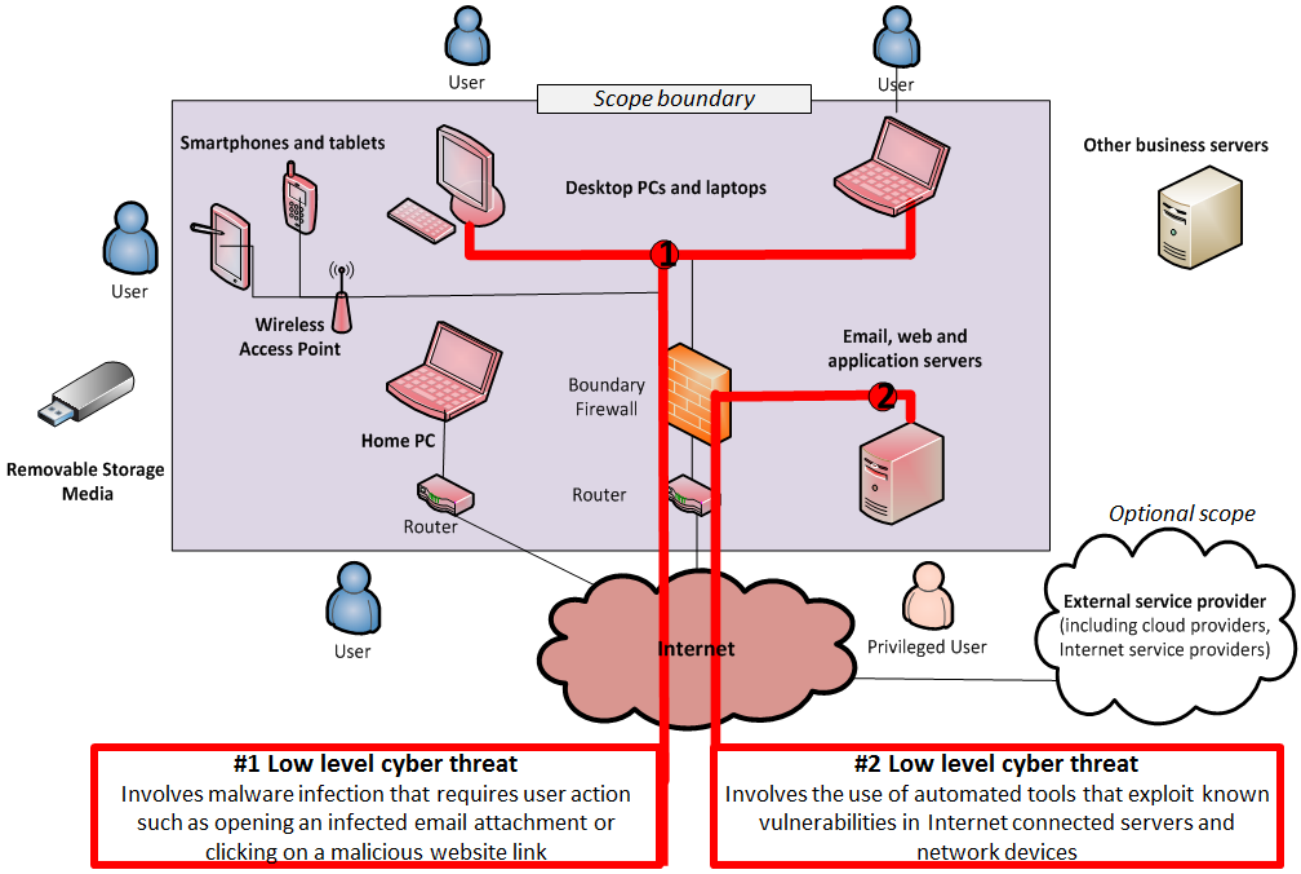
- Identified the scope subject to certification.
- Understood the Cyber Essentials requirements.
- Asserted their compliance with the Cyber Essentials requirements.
- A reasonable prospect of passing the tests for Cyber Essentials Plus.

For Cyber Essentials Plus, the certification process shall include independent testing of whether the controls implemented collectively defeat threats from hacking and phishing. The testing shall cover all Internet gateways, all servers providing services directly to unauthenticated Internet based users and user devices representative of 90% of all user devices.

Certification Bodies

A Certification Body is a company that has been accredited by an Accreditation Body to assess and certify organisations against the Cyber Essentials requirements document. A company can only become a certifying body if it meets the requirements set by its Accreditation Body including access to one or more individuals that hold the required assessors' qualifications.

Scoping



Scope of the requirements for basic technical protection

Boundary of Scope

Certification can cover the whole of an organisation's enterprise IT as illustrated above, or a sub-set. Whether the whole or a part of the organisation is subject to certification, the boundary of the part in scope must be clearly defined in terms of the organisation or business unit managing it, the network boundary and physical location. The name on the certificate must be consistent with the scope. Cyber Essentials is not intended for use with bespoke IT systems such as those found in manufacturing, industrial control systems, on-line retail and other environments.. Whilst the fundamentals of Cyber Essentials are equally applicable, these types of system will have different constraints, attack vectors and vulnerabilities.

Cloud Services

Many organisations use cloud services or other externally provided IT services. Where application of the Cyber Essentials control requirements remains under the control of the organisation seeking certification, then those requirements shall be in scope of certification. For example, an organisation which has procured infrastructure as a service from a cloud service provider and has control of the operating system on IT equipment subject to phishing or hacking threats, their secure configuration, user access control, malware protection and patch management shall be in the scope of certification.

Organisations can choose whether to include within the scope of certification Cyber Essentials control requirements that are under the control of the service provider. The certificate shall state if externally provided IT services are used and whether they are in scope. If an organisation includes externally provided IT services within the scope of a Cyber Essentials assessment then:

- For Cyber Essentials, the organisation will need to attest that its service provider's system delivering that service meets the Cyber Essentials requirements for which the service provider is responsible. Existing evidence (such as that provided through PCI certification of a cloud service and appropriately scoped ISO 27001 certifications) may be considered as part this process.

- For Cyber Essentials Plus, the organisation will need to ensure that its service provider's system delivering that service is tested as meeting the Cyber Essentials requirements for which the service provider is responsible.

Bring Your Own Device (BYOD)

BYODs are in scope. A number of the controls identified in the requirements document will need to be implemented on user devices across the organisation. This has traditionally been done through centralised administration, ensuring consistency across the organisations user estate. Certification of the security controls in such an environment is straightforward as there will usually be a standard build or reference that can be assessed. Consistency can still be achieved within a BYOD regime, however as users are given more freedom to 'customise' their experience, there is a risk that certification (and implementation of controls) will become more challenging, and potentially more expensive. This risk will also be monitored closely as the assurance framework develops.

Web Applications

Commercial-Off-The-Shelf products that support web applications which are publicly accessible from the Internet, including by open registration, are by default in scope. Bespoke and custom components of web applications are out of scope for Cyber Essentials as the scheme is not intended to identify implementation vulnerabilities. Whilst these may be identified by commodity capabilities, the exploitation of the host system (as opposed to the browsers of visiting users by Cross Site Scripting) through these vulnerabilities goes beyond the basic level of capability Cyber Essentials is intended to mitigate. The primary mitigation for these types of vulnerability is robust development and testing in line with commercial best practice such as the OWASP standards.

Contact us

For more information on this assurance framework or to apply to be an Accreditation Body, please contact cyberessentials@cesg.gsi.gov.uk.

This publication is also available on our website at www.bis.gov.uk

Any written enquiries regarding this publication may be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/15/72