

An Introduction to Cyber Essentials Certification

Business Information Factsheet
BIF538 · August 2017

Introduction

Cyber Essentials is a cyber security certification scheme that aims to help organisations prove a good baseline of cyber security and can assist in identifying the basic processes and procedures needed to protect against cyber-attacks.

This factsheet outlines the requirements and standards that Cyber Essentials certification requires of organisations. It explains the five key areas of controls, provides information on the steps to achieving certification and the benefits of doing so.

What is Cyber Essentials?

Cyber Essentials is the government-backed cyber security certification scheme for small firms. Its goal is to set out the basics of cyber security and guide firms through the process of self-protection against cyber security risks.

Cyber Essentials covers all the basic security weaknesses that an organisation might have within its own IT systems and software. It works on the basis that straightforward but robust measures can have a big impact when it comes to external cyber security risks.

To develop the Cyber Essentials scheme, the UK Government worked in collaboration with relevant industry bodies such as the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI).

What are the benefits of Cyber Essentials certification?

There are a number of benefits for small firms who achieve Cyber Essentials certification:

- **Demonstrating resilience:** a business can promote cyber security as one of its core strengths when dealing with clients, insurers and investors.
- **Increasing commercial opportunities:** firms can bid for public sector contracts and offer robust cyber security protocols as a standard when pitching for work.
- **Saving money:** organisations with Cyber Essentials certification are considered by insurers to be less susceptible to cyber-attack. This could be reflected in reduced insurance premiums.
- **As a basis for other security-related issues:** Cyber Essentials provides a starting point for compliance with the Data Protection Act 1998 (and the forthcoming General Data Protection Regulation from May 2018). It also forms the basis for broader information security governance as set out by the national Cyber Security Centre.

What cyber security controls does it address?

Cyber Essentials certification requires organisations to have five technical controls in place:

- **Secure network configuration:** Computers and network devices need to be securely and properly configured. The assessment process can help identify any systems or procedures that do not adhere to standard levels of protection against use of unused software, weak passwords or auto-run programs.
- **Malware protection:** This is a tool that helps in the prevention of a computer being infected with malicious software, including spyware, viruses, worms and other code that can cause harm. Any software used for malware protection and virus removal should be updated frequently to ensure that the latest protection is being used.
- **Boundary firewalls and internet gateways:** Boundary firewalls block attackers and other external threats. They also mean that external traffic trying to access network servers can be better monitored and managed.
- **Access control and administrative privilege management:** Proper management of access control, administrative privileges and passwords helps prevent any insider threats, deliberate or accidental.
- **Patch management:** Regular software patching and licensing updates ensures security and optimal software performance and also minimises the risk of systems becoming redundant.

What is the accreditation process?

Organisations can choose any official accreditation body to manage their Cyber Essentials certification. There are currently five official Cyber Essentials accreditation bodies that are appointed by the Government:

- APMG International (www.apmg-cyber.com).
- CREST (International) (www.crest-approved.org/cyber-essentials/index.html).
- Information Assurance for Small and Medium Enterprises Consortium (IASME, www.iasme.co.uk/cyberessentials/).
- IRM (www.irmsecurity.com).
- QG Business Solutions (www.qgstandards.co.uk).

There are two levels of Cyber Essentials certification available - Cyber Essentials and Cyber Essentials Plus.

The basic Cyber Essentials certification process costs between £300 and £400 and involves the completion of a self-assessment questionnaire which is then validated by the accreditation body. Cyber Essentials Plus certification is more expensive and requires an additional on-site system review and assessment.

Once a self-assessment questionnaire has been completed, it is reviewed by the accreditation body. The accreditation body will provide feedback on the answers provided in the questionnaire and highlight if there are any issues that need to be addressed. Once the accreditation body is satisfied that the organisation has fulfilled all the requirements, they will approve the certification.

The accreditation body will send the official certificate, along with brand guidelines for including the Cyber Essentials Certification logo on the organisation's website or promotional materials.

Cyber Essentials certification lasts for a period of 12 months and then organisations must seek recertification. The process for recertification is the same, but organisations need to be aware that the certified accreditation bodies might change from year to year, as might the requirements for certification.

Further information

BIF536 A Guide to the General Data Protection Regulation (GDPR)

Useful publications

'Cyber Essentials Scheme: Overview'

Website: www.gov.uk/government/publications/cyber-essentials-scheme-overview

Useful contacts

Cyber Aware is a cross-government campaign delivered by the Home Office.

Website: www.cyberaware.gov.uk

DISCLAIMER While all reasonable efforts have been made, the publisher makes no warranties that this information is accurate and up-to-date and will not be responsible for any errors or omissions in the information nor any consequences of any errors or omissions. Professional advice should be sought where appropriate.

Cobweb Information Ltd, Unit 9 Bankside, The Watermark, Gateshead, NE11 9SY.

Tel: 0191 461 8000 Website: www.cobwebinfo.com