A guide to starting Cyber Essentials

TABLE OF CONTENTS

InfoSec GOVERNANCE LTD

What is Cyber Essentials?

Cyber Essentials is a UK government backed cyber security scheme which has been designed to protect businesses of all sizes from internet based threats.

Cyber Essentials is an annual certification which means you must renew your certification every 12 months or lose your certification. The achievment of Cyber Essentials is a requirement to provide services to the central government, NHS and the Ministry of Defence.

The scheme is made up of five primary technical controls which cover all aspects of your IT within the business. From ensuring that you patch and keep systems up to date, are not running as a local administrator, to ensuring that anti-malware software is installed and updated.

By achieving Cyber Essentials you will be:

- Reassuring your customers, suppliers and partners that you are working to secure your business against cyber attacks
- Winning business through showing your willingness to protect information
- Be able to work with Government departments by complying with contractual agreements

The Cyber Essential scheme come in two levels, the basic self-assessment and then the more in depth Cyber Essentials Plus, which audits you against your basic certification.

The Cyber Essentials basic certification is a self-assessment certification which is completed on an online portal and is then marked.

The Cyber Essentials Plus audit is an onsite or remote based audit which validates the controls from the self-assessment certification.

Who is NCSC?

The National Cyber Security Centre (NCSC) is part of the UK Government who's purpose is to provide advice and support for the public and private sector in how to avoid computer security threats.

NCSC own the overall Cyber Essentials Scheme and are based in London. The parent business is the Government Communications Headquarters (GCHQ).

Who is IASME?

The IASME Consortium, more commonly known as IASME, are the certified partners of the Cyber Essentials Scheme. They manage the day-to-day running of the scheme for NCSC. IASME issue the Cyber Essentials certifications with the help of Certification Bodies, like InfoSec Governance.

IASME also have their own Information Security standard, called IASME Cyber Assurance, which can be seen as a stepping stone towards the ISO 27001 journey.

How much does it cost?

The cost of Cyber Essentials is based upon a standard pricing tier that is provided by the NCSC and IASME and is based upon the number of employees within the business.

This cost will cover the cost of being setup within the online portal, a free pre-submission review (through InfoSec Governance) and the issuing of your certification (upon successful completion).

Business Size	Price
Micro (0 - 9 Employees)	£320 + VAT
Small (10 - 49 Employees)	£440 + VAT
Medium (50 - 249 Employees)	£500 + VAT
Large (250 employees and above)	£600 + VAT

Free Cyber Liability insurance up to £25,000 is available within this pricing for any business that is domiciled with the UK and turns over less than £20 million.

The Cyber Essentials scheme doesn't expect businesses to have to purchase additional technology and services to comply with the technical controls and achieve certification. However, you must ensure full compliance.

The five technical controls

Within the Cyber Essentials scheme, there are five core technical controls that must be implemented within the business to ensure you fully comply.

These controls are the same for every business whether a micro or enterprise.

Firewalls

You must ensure that there are software firewalls enabled and configured on all endpoints. If working in a business environment, you must have border firewalls to protect and separate from the internet.

Firewalls should be configured to block all incoming communication by default and only allow traffic in when there is a documented business case.

Secure Configuration

You must ensure that default administrative credentials are changed to something new. That all computers should have unused and unsupported applications removed and unnecessary services removed.

Security Update Management

All Operating Systems, applications, libraries etc.. must be kept up to date and any high or critical updates applied within 14 days of release from the vendor.

User Access Control

Users should only be granted access to the systems, shares and processes for what they need (least privilege access).

Malware Protection

Anti-malware software should be implemented and kept up to date at all times. Anti-malware software should be applied on all end user devices, including servers.

Currently under Cyber Essentials there is no known anti-malware software for mobile devices, this should be configured with application approvals.

The certification process

If you would like to progress with the certification to Cyber Essentials, the process has been made as simple as possible.

1. You contact InfoSec Governance to ask about Cyber Essentials, you provide the number of employees within the business.
2. InfoSec Governance provide a quotation to provide Cyber Essentials to your business.
3. You accept the quotation
4. InfoSec Governance ask you for the following information:
    a. Name of company
    b. Company registered address
    c. Name of person who will complete the self-assessment
    d. Email address of person who will complete the self-assessment
    e. Mobile number of person who will complete the self-assessment, this is for the portal password.
    f. Purchase Order number (if required)
5. You provide the necessary information
6. InfoSec Governance setup access to the online Cyber Essentials portal and an invoice is sent out (payable within 30 days)
7. You complete all the answers within the portal, then when finished notify InfoSec Governance before submission
8. InfoSec Governance review answers and provide any guidance if required.
9. You update any answers, if needed
10. InfoSec Governance certify the business to Cyber Essentials
11. InfoSec Governance get back in touch 11 months later to remind you to re-certify

Frequently Asked Questions

Do I have to apply all the technical controls to my business?
Yes, the five technical controls must be applied, otherwise you will not be successful in certification.

Are personal devices (BYOD) part of the scheme?
If personal mobile devices access any business data or services (such as email, support tickets etc.), then these are in scope of the assessment.

Are cloud services in scope of the assessment?
All cloud services, such as Microsoft 365, Google Workspace, Xero, Amazon AWS are all in scope if used.

Do I have to apply updates with in 14 days?
Yes, all high and critical security updates must be applied within 14 days of release by the manufacturer.

What if my developer needs to run as a local administrator?
The developers will have to have account separation and use a standard user account for their day-to-day usage. There should be no reason why they should have to run as a administrator account.

Does everyone need multi-factor authentication for cloud services?
Yes, all users and administrators must have multi-factor authentication enabled for all cloud services. If this is not possible you will receive some major non-compliances.

I can find Cyber Essentials cheaper, will you match the price?
No, our prices are set as in this document.

0330 043 0826 | info@isgovern.com | https://isgovern.com

InfoSec Governance Ltd is a registered company in England & Wales (12289766).
Registered office: 73 Duke Street, Darlington, DL3 7SD