

Cyber Essentials Certification

All you need to know...



**HALIFAX
COMPUTERS**



Cyber Essentials in a Nutshell

Cyber Security is not to be taken lightly by any business due to the consequences and potential fines regarding data leaks. The Cyber Essentials scheme is a Government backed, industry recognised certification that is perfectly suited to any business looking to build a solid foundation in Cyber Security.

Cyber Essentials enables all UK businesses to adhere to a series of Cyber Security principles that safeguard their business data and clients data. They can also participate in high value tenders that require this certification. Unlike other Cyber Security schemes, that are not Government backed, Cyber Essentials is very affordable and well recognised across all industries.

Cyber Essentials helps businesses to mitigate against phishing attacks including; malware, malicious email, website links and hacking. This is undertaken by exploring the known vulnerabilities in the internet connected server and devices during the audit process. Risks are identified and recommendations are then made in-line with the certification criteria.

The Cyber Essentials Certification Framework

Within the two Cyber Essential's certification options, the following five security controls are verified.

- 1. Boundary firewalls and internet gateways**
- 2. Secure configuration**
- 3. Access control**
- 4. Malware protection**
- 5. Patch management**

Why Cyber Essentials?

Properly implemented cyber security has the additional advantage of driving business efficiency throughout the organisation, saving money and improving productivity. The five security controls that form the framework of both Cyber Essentials certifications prevent around 80% of cyber attacks*.

Core Benefits



Tender Requirements

As cyber security is such an important factor of any business setup, many larger tenders now specify a Cyber Essentials certification as part of the standard submission criteria.



Risk Mitigation

Cyber Essentials helps businesses identify risks they face when it comes to cyber security. In order to achieve certification, there needs to be specific processes and structures in place to combat these risks.



Data Protection

At present, data protection is regulated by the Data Protection Act 1998. However, within the next two years the EU General Data Protection Regulation (GDPR) will come into force. Business owners are now solely responsible for the security of clients' data in line with the new regulation. Cyber Essentials helps identify weaknesses and puts processes in place to protect data.



Protection from Cyber Threats

Thousands of businesses every year fall victim to cyber security attacks which cost time, money and potentially the loss of company and client data. Cyber Essentials ensures cyber security processes are in place to help prevent these attacks.



Stand Alone Assurance

Broader standards and frameworks provide a different level of cyber security. Cyber Essentials is a stand-alone assurance programme that is most appropriate for organisations for whom IT is a business enabler rather than a core deliverable.

* Stat source: UK Government Data via www.gov.uk

What's Covered in the Certifications?

1: Boundary Firewalls and Internet Gateways

Using boundary firewalls to monitor traffic to your server(s) enables you to better understand and manage your bandwidth requirements, which can block attackers and external threats.

2: Secure Configuration

By ensuring your computers and network devices are configured properly, you can identify systems or databases that you no longer need or use. This will give you the opportunity to reduce your overall storage and bandwidth consumption, as well as reducing the level of inherent security vulnerabilities.

3: Access Control and Administrative Privilege Management

Managing access control and administrative privileges erodes the opportunity for staff to install time-wasting software onto their computers, as well as removing the insider threat.

4: Malware Protection

Implementing appropriate malware protection has its obvious security advantages, but an often overlooked hidden benefit is the time and cost savings that result from avoiding devices being out of action.

5: Patch Management

Keeping on top of software patching and licensing makes your company more productive, as well as more secure. Patches improve the performance of the products they apply to, and remove issues that slow down employees, such as crashes and poor performance caused by congested networks.

How is the Plus Different?

This certification is more comprehensive and is awarded by Crest - an accredited Certification Body - after validation. The Cyber Essentials Standard is a self-certified certification.



The two Types of Certification

Cyber Essentials Standard

CYBER
ESSENTIALS



This affordable certification is awarded on the basis of a verified self-assessment. However, to achieve this the business needs to put in place a series of detailed policies and processes which take time to assess and implement. Our partner helps businesses to then undertake their own assessment via the online self-certified questionnaire. This questionnaire is then verified by one of our partner's independent Assessors to confirm whether the certification criteria has been achieved. Cyber Essentials Standard is then awarded as a result if they pass.

Ideal for Businesses who:

- ✓ **Want to demonstrate Government backed IT Security compliance**
- ✓ **Are keen to then obtain the Cyber Essentials Plus Certification**
- ✓ **Are looking to work towards, or want an addition to, ISO 27001**

Cyber Essentials Plus

CYBER
ESSENTIALS
PLUS



The Cyber Essentials Plus certification can only be obtained by a business after the Cyber Essentials Standard has been awarded. This fully audited certification is awarded by an external Certification Body and offers a higher level of assurance through the external testing of the businesses cyber security approach. A thorough security scan of the network is undertaken by our partner and all vulnerabilities are identified.

Ideal for Businesses who:



- ✓ **Want to tender for large value projects**
- ✓ **Work within highly regulated industries**
- ✓ **Are looking to work towards, or want an addition to, ISO 27001**

Cyber Essentials Package Prices

The Cyber Essentials Standard is a prerequisite to Cyber Essentials Plus, which provides a more thorough assessment via Crest, the official Certifying Body.

Our Cyber Essentials partner offer affordable packages for both the Standard and Plus.

What's included?	Cyber Essentials Standard	Cyber Essentials Plus
Basic on-site audit undertaken by a Cyber Security Specialist	✓	✓
Detailed report outlining your performance against the Cyber Essentials framework	✓	✓
A list of recommended actions to be completed within 4 weeks of the audit	✓	✓
Online Cyber Essentials questionnaire submission for verification	✓	✓
Comprehensive on-site audit undertaken by Crest accreditor		✓
On-site verification visit by Crest accreditor and certification awarded		✓

	Company Size			
	0-50 staff	51-100 staff	101-150 staff	over 150 staff
	POA	POA	POA	POA
	POA	POA	POA	POA

NB: Additional work in order to meet the recommendations outlined in the report findings are not included in the above prices and will be quoted separately if required.

FAQs & ISO 27001

How is Cyber Essentials Different to ISO 27001?

ISO 27001 is a comprehensive industry standard that enables businesses to tender and work on large projects. Achieving it, demonstrates that your business assesses and prevents security risks.

It can take a long time for businesses to put in place the processes and frameworks required to meet the ISO 27001 standard and therefore it's much more expensive to achieve than the Cyber Essentials certification.

The Role of Cyber Essentials

The Cyber Essentials certification is perfect for businesses looking for a stepping stone to ISO 27001 or an addition to ISO 27001. Having the Cyber Essentials certification gives your business a head start over anyone planning to achieve ISO 27001 from scratch as given the standard is based on ISO 27001 to begin with, adopting it's 'big brother' will be more straight-forward.

For businesses who already hold ISO 27001, Cyber Essentials is regarded as a complimentary addition.

How do ISO 27001 and Cyber Essentials Compare?

Cyber Essentials is not directly comparable to ISO 27001 because it is not as comprehensive. The Cyber Essentials framework (that applies to both Plus and Standard is explained in detail on page 4).

Do Businesses Need Both ISO 27001 and Cyber Essentials Certification?

The short answer is yes. Previously for a business to tender for large projects they needed to have the ISO 27001 to meet the submission criteria. However, it is now common practice that the Cyber Essentials certification is also a requirement.



**HALIFAX
COMPUTERS**

Tel: 01422 25 77 77
sales@halifaxcomputers.co.uk
www.halifaxcomputers.co.uk