CREST has a large number of Certifying Bodies whose details are available on both the Cyber Essentials website – **www.cyberessentials.org** – and on the CREST website – **www.crest-approved.org** - which also profiles each company to help organisations make their selection and move to formally appoint.

How it works

	CYBER ESSENTIALS	CYBER ESSENTIALS PLUS
Self-assessment questionnaire	✓	✓
External vulnerability scan*	✓	✓
Internal vulnerability scan and on-site assessment		✓

Delivered by CREST-accredited Certification Bodies

Further Information

The following additional information is available from **www.cyberessentials.org**:

- A comprehensive Guide to the Cyber Essentials scheme
- Cyber Essentials Common Questionnaire
- Cyber Essentials Plus Common Test Specification
- CREST member companies providing Cyber Essentials certification services
- Short awareness training courses

CREST (GB) Ltd, Abbey House, 18-24 Stoke Road, Slough, Berkshire SL2 5AG
Tel: 020 3058 3122 email: info@cyberessentials.org www.crest-approved.org www.cyberessentials.org

CYBER ESSENTIALS: An Overview

A primary objective of the UK Government's National Cyber Security Strategy is to make the UK a safer place to do business.

Cyber Essentials is a cyber security standard that uses independent assessment to identify the IT security controls that an organisation needs to have in place to have confidence that they are addressing cyber security effectively and mitigating the risk from internet-borne threats. An organisation's technology that is exposed to common cyber-attacks will typically include internet connected computers, such as desktop PCs, laptops, tablets and smartphones, along with internet connected servers such as email, web and application servers.

About Cyber Essentials

The Cyber Essentials scheme focuses on the following five essential mitigation strategies:

Secure configuration

Boundary firewalls and internet gateways

Access control and administrative privilege management

Patch management

Malware protection

The scheme provides organisations with clear guidance on implementation, as well as offering independent certification for those who want it. After certification, an organisation is able to demonstrate to customers that its data is adequately protected and that it takes cyber security seriously. There are two levels of certification:

- Cyber Essentials - organisations complete a self-assessment questionnaire which is reviewed by an external Certifying Body
- Cyber Essentials Plus - tests of the organisation's systems are carried out by an external Certifying Body

An overview of them is described below.

Getting your Business Certified

Both Cyber Essentials and Cyber Essentials PLUS include a questionnaire which relates to security controls and the secure configuration of an organisation's computing resources. CREST Certifying Bodies also conduct an external vulnerability scan as part of a remote technical assessment at the Cyber Essentials level. This provides organisations with independent validation of elements of the questionnaire.

The key differentiator for Cyber Essentials PLUS is the inclusion of a technical review of the organisation's workstations. This additional phase of testing increases the validity of certification considerably by providing evidence of compliance against the following scenarios:

- Can malicious files enter the organisation from the Internet through either web traffic or email messages?
- Should malicious content enter the organisation, how effective are the anti-virus and malware protection mechanisms?
- Should the organisation's protection mechanisms fail, how likely is it that the organisation will be compromised due to failings in the patching of the organisation's workstations?

Cyber Essentials PLUS is a more thorough assessment of the organisation and, as a result, provides greater security assurance. However, it does come at an additional cost, which will factor into the decision making process. Ultimately the decision on which level to certify against is influenced by an organisation's cyber security stance and those of its business partners, suppliers and stakeholders.

Once an organisation is assessed against the Cyber Essentials security criteria and passes, it will receive the relevant Cyber Essentials award (badge) based on the level of certification achieved. This demonstrates that it has achieved a fundamental level of cyber security.

Appointing a Certifying Body to carry out the assessment

Once a decision has been reached to proceed with a Cyber Essentials certification, a Certifying Body must be appointed to carry out the assessment. Organisations have a number of suppliers to choose from. Value can be gained by appointing a supplier who is certified and possesses accredited consultants because the combination of these features provide an organisation with the greatest assurance and confidence that an effective and professional assessment has been performed. Many organisations, however, face a challenge in identifying trusted suppliers that have access to competent, qualified experts.

CREST is a not-for-profit accreditation body whose role is to create and maintain high standards within the cyber security sector and to drive a consistency of quality across its member organisations to offer assurance to the buying community.

Any organisation procuring Cyber Essentials services can be assured that CREST Cyber Essentials Certifying Bodies have:

- Demonstrated appropriate levels of quality assurance processes, security controls, security assessment methodologies and met additional qualification criteria
- Proven access to technically competent and qualified staff
- Committed to abiding to the requirements of Certification Bodies for Cyber Essentials
- Signed an enforceable Code of Conduct

In addition to Cyber Essentials certification services, CREST Certifying Bodies also provide a range of other services to help organisations better manage their cyber security risks. These include:

- Penetration testing
- Security audit and compliance
- Security policy
- Security architecture
- Cyber security incident response
- Threat intelligence

This takes away much of the stress in validating the competence of the cyber security assessors and almost certainly ensures a faster route to certification.

Any Certifying Body will be able to talk through the requirements and scoping necessary for Cyber Essentials or Cyber Essentials Plus assessments and help organisations to understand their options.