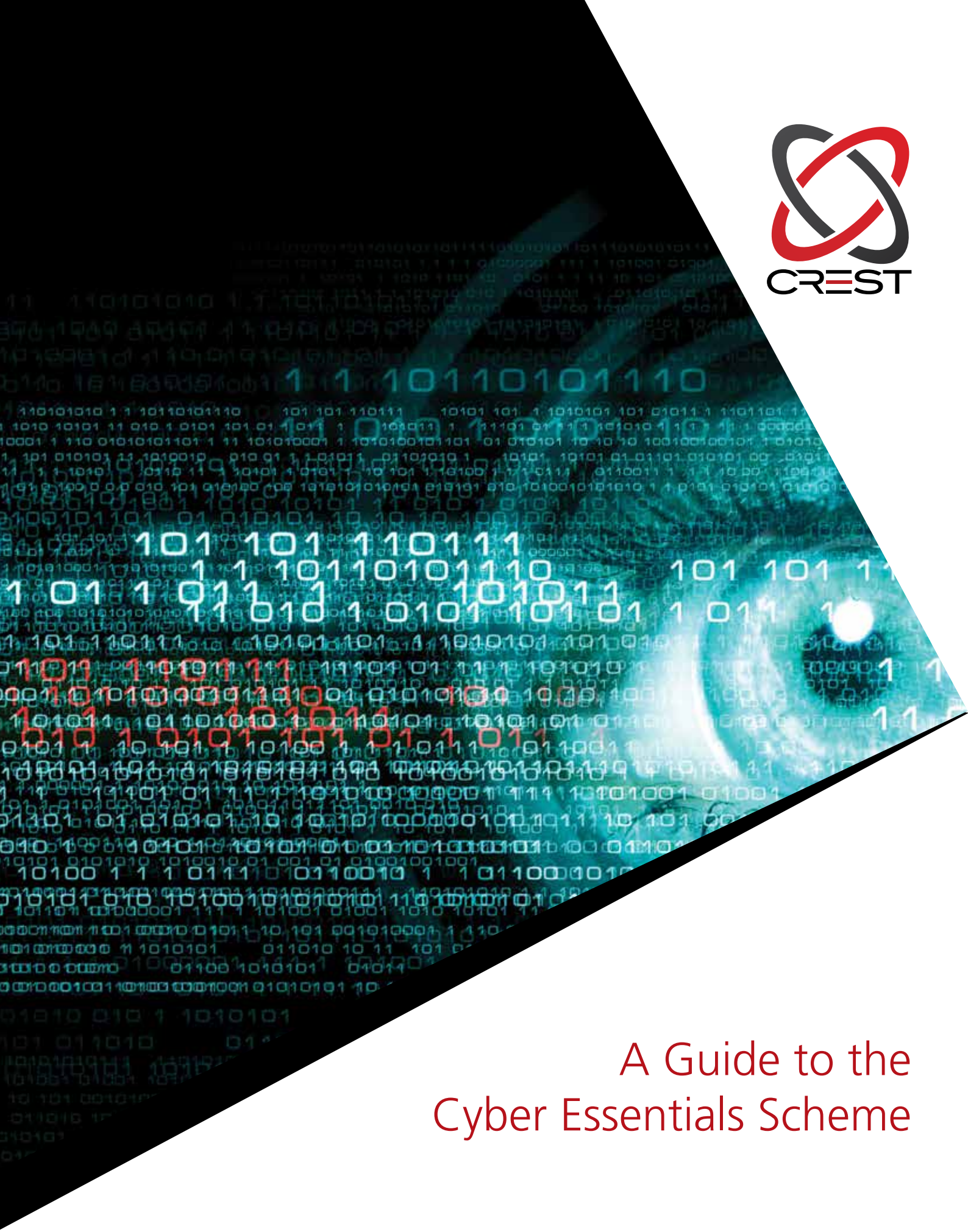


CREST

A Guide to the Cyber Essentials Scheme

CYBER ESSENTIALS

Published by:

CREST

Tel: 0845 686-5542

Email: **admin@crest-approved.org**

Web: **http://www.crest-approved.org/**

http://www.cyberessentials.org/

Principal Author

Jane Frankland,

Managing Director, Jane Frankland Agency

Principal reviewer

Ian Glover, President,

CREST

Acknowledgements

CREST would like to extend its special thanks to those CREST member organisations that took part in this project, and contributed to the production of this Guide.

Warning

This Guide has been produced with care and to the best of our ability. CREST accepts no responsibility for any problems or incidents arising from its use.

About this Guide

This Guide provides practical advice for organisations that are looking to improve their basic cyber security controls and achieve a cyber security certification. It has been designed to meet the requirements of organisations within the commercial, not-for-profit and public sectors and for individuals who are responsible for mitigating cyber risk and enabling business within their organisations.

This Guide provides a short overview of the background to the scheme and the benefits associated with certification. It is of particular relevance to small-to-medium sized enterprises (SME's) whose IT systems are primarily made up of common-off-the-shelf (COTS) products, rather than heavily customised, complex solutions, and where IT is a business enabler rather than a core deliverable.

An Introduction to the Cyber Essentials Scheme

In 2012, HM Government launched the 10 Steps to Cyber Security guide to encourage organisations to consider their cyber security measures, and to ascertain whether organisations thought they were managing their cyber risks sufficiently. The guide was extremely well received, and raised awareness within company boards and amongst senior executives. Business leaders were encouraged to take ownership of their cyber risks and to build them into their overall corporate risk management regime.

Whilst the initiative gained good traction, HM Government's analysis of continuing cyber attacks, and feedback from the cyber security industry at large, was that a number of security controls were still not being implemented effectively. This posed a concern for HM Government. With a remit to tackle cyber crime and a desire to make the UK one of the most secure places in the world to do business in cyberspace, it was clear to HM Government that further initiatives were required.

The adoption of an organisational standard for cyber security was therefore seen as the next step on from the 10 Steps to Cyber Security guide. The rationale behind this was that it would enable organisations and their customers and partners, to have greater confidence in their ability to measure and reduce basic cyber risks, as they would be independently assessed, where necessary.

HM Government, together with industry, instigated a call for evidence on a preferred organisational standard in cyber security. Concluding in November 2013, the feedback received was that none of the existing standards for cyber security met the specific requirements identified, and that industry was prepared to help HM Government develop something more appropriate. The new requirements have now been embedded in the Cyber Essentials scheme.

The Cyber Essentials scheme defines a basic cyber security standard, which organisations can be certified against. It identifies the security controls that organisations must have in place within their IT systems in order to have confidence that, at a basic level, they are addressing cyber security effectively and mitigating most commonly seen risks from Internet-based threats.

The scheme focuses on five essential mitigation strategies within the context of the 10 Steps to Cyber Security guide. It provides organisations with clear guidance on implementation as well as offering independent certification for those organisations that want it.

Whilst providing a basic but essential level of protection, the Cyber Essentials scheme provides a metric against which organisations can measure their level of cyber security maturity. For those organisations that believe that they are practicing good cyber security it provides a certificate that can be used to demonstrate to customers and business partners that they have in place industry recognised minimum standards.

Cyber Essentials and Good Security Practice

Achieving a strong cyber security posture can consume significant amounts of time, money, and human resource, and implementing good security practices is paramount for organisations with data to secure. The first place to begin is to consider an organisation's key information assets, related systems and risks. By identifying the risks that an organisation faces, the selection of its security practices, controls and, if necessary, the certifications and standards by which it will align, will become more apparent.

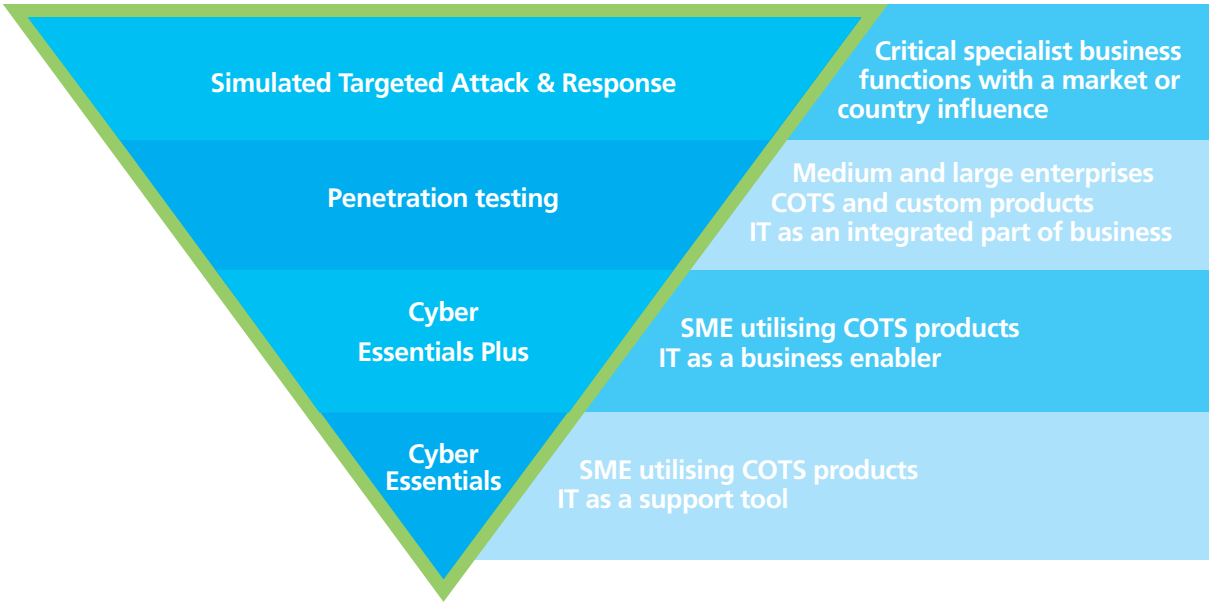
Each organisation will have a unique risk profile. For an organisation to gain an appropriate level of assurance it should implement a range of cyber security controls and, alongside Cyber Essentials, may need to consider the requirements of broader standards and frameworks, such as ISO 27001, PCI, COBIT, or the ISF Standard of Good Practice.

The Cyber Essentials scheme provides a well-defined standard and is appropriate for organisations that seek to demonstrate a base level cyber security certification. Cyber Essentials as a stand-alone assurance programme is most appropriate for organisations for whom IT is a business enabler rather than a core deliverable. As has been stated, it is relevant to organisations whose IT systems are primarily made up of common-off-the-shelf (COTS) products, rather than heavily customised, complex solutions.

The scheme represents an industry recognised approach for an organisation to take if it wants a standalone activity and does not have a high-risk environment to secure. However, it must be placed in the context of all good security management practice. For example, it can be used as grounding for other activities such as penetration testing where the review is more in-depth and the actual vulnerability is tested against defined and real threats.

The same goes for an organisation that has a requirement to be PCI DSS and or ISO 27001 certified. Whereby all of these standards share similar ideologies, the approaches taken are different. For example, ISO 27001 is voluntary, and an overall measure for an organisation to use for compliance of information security management. PCI DSS, on the other hand, is mandated and is a more standardised and regulated sub-section of information security management that pertains specifically to cardholder data.

As is apparent, managing cyber security is a complex task for any organisation. The best approach to take is to seek the guidance of the experienced Cyber Essentials Certification Bodies. In addition to providing advice on the most appropriate standards they can perform a security review and/or risk assessment and help the organisation to determine which activities, controls, practices and certifications are right for mitigating the risks within their unique environment.



Why put your Organisation through Cyber Essentials Certification?

Cyberspace is changing the way we conduct business, and as a result it can bring huge benefits along with higher levels of risk exposure. As events in cyberspace can happen at any time, from any location and with immense speed many organisations operate at risk, unaware of the dangers associated with this new dependence on cyberspace. Intellectual property and other commercially sensitive information, such as business strategies, can be attractive targets for cyber criminals. Equally, services relying on, or delivered via, cyberspace can be taken offline by attackers, damaging revenue and reputations.

Achieving a certification in a scheme such as Cyber Essentials provides an organisation with sound, commercially viable benefits. Through independent assessment, organisations of all sizes can have the confidence that they are addressing basic cyber security effectively, mitigating certain risks from Internet-based threats and better protecting their assets.

The scheme provides a benchmark for Cyber Essentials certification providers to meet, that includes the need to provide a quality and consistent service, and takes into account the requirements to protect client information. Underpinned by meaningful and enforceable codes of conduct, these two elements deliver a high degree of protection to buyers, and enable supplier selection with high levels of confidence.

Organisations that possess a Cyber Essentials certification can gain a business advantage, as potential customers view them as organisations with sound cyber security practices. By using processes and controls to ensure higher levels of assurance, organisations are able to consistently satisfy their customers that their Internet facing systems are relatively secure. Certification, therefore, can serve as a powerful marketing tool, and can provide a significant competitive edge, especially if an organisation is early to implement it in their industry.

With more attention being placed on cyber security, and as threats increase and data breaches hit the headlines, many customers, including corporates and government agencies, are asking suppliers to provide evidence that validates their security posture. Typically this means supplying an independent assessment report or by demonstrating relevant industry certification. If a supplier is unable to do this, it can put them at a competitive disadvantage.

Until recently, achieving a certification in cyber security was out of reach for small organisations. In terms of cost and time. The Cyber Essentials scheme now makes this achievable by offering a lower cost and more accessible solution for small organisations seeking cyber security certification.

What is Involved in the Certification Process?

The first stage in the certification process is to decide which level to certify against – Cyber Essentials or Cyber Essentials Plus. Although there are only two certifications to consider now, an organisation should be aware that future levels are planned, with an aim to further entrench the scheme into an organisation's over-arching approach to information risk management, such as ISO 27001 and in accordance with the 10 Steps to Cyber Security.

Once an organisation has been assessed against the Cyber Essentials security criteria and passes, they will receive the relevant Cyber Essentials award (badge), which demonstrates to existing and prospective customers, and other stakeholders, that they have been successfully measured against the standard.

The certification levels are described here, along with the processes an organisation needs to take.

Cyber Essentials (stage 1)

The organisation defines the scope, which is made up of the systems that are exposed to the Internet.

The organisation states its compliance with the requirements by responding to the Cyber Essentials questionnaire, which covers the requirements for basic technical protection from cyber attacks. To complete the process, an authorised signatory of the organisation signs the questionnaire attesting its accuracy. This is then sent to a recognised body for review.

The organisation also undergoes an external vulnerability assessment from the certifying body. This directly tests that individual controls on the Internet facing network perimeter have been implemented correctly, and that obvious vulnerabilities are not present.

Certification at this level should be seen as a snapshot of the organisation or system at the time of assessment. It does not provide assurance that the controls will continue to be implemented correctly, or that systems are effectively configured to defend against more targeted, sophisticated or persistent attacks.

Cyber Essentials Plus (stage 2)

Having completed Cyber Essentials stage 1, which is a prerequisite to Cyber Essentials Plus (stage 2), an organisation may choose to undergo a more thorough assessment from a certifying body. This time the assessment is based on an internal security assessment of end-user devices. Once again this directly tests that individual controls have been implemented correctly and recreates various attack scenarios to determine whether a system compromise using basic capabilities can be achieved.

Certification at this level should again be seen as a snapshot of the organisation or system at the time of assessment. It does not provide assurances that the controls will continue to be implemented correctly, or that systems are effectively configured to defend against more targeted, sophisticated or persistent attacks.

How to Start the Certification Process

Once a decision has been reached to proceed with a Cyber Essentials certification, a certifying body must be appointed. Organisations have a number of suppliers that they can select, from an approved list.

CREST member companies are ideally placed to meet these requirements. By appointing a CREST member company, an organisation can rest assured that they are procuring cyber security services from a trusted, certified external company that employs professional, ethical and highly technically competent individuals. This takes away the challenge and cost of validating the competence of the cyber security assessors, and certainly ensures a faster route to certification.

An organisation can access certified suppliers via the CREST website, **www.crest-approved.org** or the CREST website for Cyber Essentials, **www.cyberessentials.org**, where further information can be found about the scheme and links to the approved certification bodies' websites. After evaluating the suppliers, an organisation can then make their selection and move to formally appoint. An organisation should make sure that their chosen supplier not only meets the specific requirements of the Cyber Essentials scheme, but for future types of assessments.

About the CREST Cyber Essentials Certifying Bodies

With threats constantly evolving, most organisations require professional help to mitigate cyber risk and to implement the right levels of cyber security. Many organisations are challenged to identify trusted suppliers that have access to competent, qualified experts.

CREST is a not-for-profit industry body, whose role is to create and maintain high standards within the technical information security industry, and to drive a consistency of quality across its member organisations.

All CREST Cyber Essentials Certifying Bodies have:

- Demonstrated appropriate levels of quality assurance processes, security controls, security assessment methodologies and met additional qualification criteria.
- Signed meaningful and enforceable Code of Conduct at a company and individual level
- Proven access to technically skilled, knowledgeable, competent and qualified staff
- Committed to abiding to the requirements of Certification Bodies for Cyber Essentials.

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

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

For further information about CREST, please visit **www.crest-approved.org**.

For further information about Cyber Essentials, please visit the CREST website for Cyber Essentials - **www.cyberessentials.org**.

Assurance In Information Security

Company Membership

Demonstrable level of assurance of processes and procedures of member organisations.

Knowledge Sharing

Production of guidance and standards.

Opportunity to share and enhance knowledge.

Professional Qualifications

Validate the knowledge, skill and competence of information security professionals.

Professional Development

Encourage talent into the market.

Provision of on-going personal development.

CREST Representation	• Demonstrable level of assurance of processes and procedures of member organisations • Not for profit • Validation of the competence of technical security staff • On-going professional development for those entering or progressing in the industry • All CREST examinations reviewed and approved by GCHQ (CESG).
CREST Penetration Testing	• Assignments performed by qualified individuals with up-to-date knowledge, skills and competencies in the latest vulnerabilities and techniques used by real attackers • Confidence that CREST Member companies will protect confidential client information.
CREST Cyber Security Incident Response (CSIR) Scheme	• Company assessments and professional qualifications endorsed by GCHQ and CPNI • Cyber Security Incident Response (CSIR) Scheme, complementing the CESG/CPNI Cyber Incident Response (CIR) Scheme • New Cyber Security Incident Response Manager's certification.
CREST Security Architects	• Professional examinations, which are formally recognised under the CESG Certified Professional Scheme.
CREST Codes of Conduct	• Provide a significant level of protection for organisations procuring technical security testing services • Ensure the quality of the services provided by, and the integrity of, both the companies and individuals involved; and enforce adherence to audited policies processes and procedures.
CREST Research	• Guidance in the form of booklets, e-books and online presentations compiled to assist the buying community, suppliers of professional services and those wishing to enter or progress in the technical information assurance industry • Work closely with e-Skills, academia and training organisations.
CREST Overseas	• Member companies in a growing number of countries, such as a formally established Chapter in Australia, which has full support of the Australian Government.

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: crest-approved.org