Business Go Digital

IT DEPARTMENT

Cyber Essentials
A guide to the scheme

CYBER ESSENTIALS

CREST

Delivered in partnership with: IT governance

Improve security

A CREST - accredited Cyber Essentials certification body will independently verify your security status.

The CREST incident response exams have all been approved by GCHQ and CPNI

CREST "Certificateless Registry for Electronic Share Transfer"

The Cyber Essentials scheme is a world-leading, cost-effective assurance mechanism for companies of all sizes to help demonstrate to customers and other stakeholders that the most important basic cyber security controls have been implemented.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. The government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it is not designed to address more advanced, targeted attacks and therefore organisations facing these threats will need to implement additional measures as part of their security strategy, such as ISO 27001.

The Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, has been designed in consultation with SMEs to be light-touch and achievable at low cost. The two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It is important to recognise that certification only provides a snapshot of the cyber security practices of the organisation at the time of assessment, and maintaining a robust cyber security stance requires additional measures, such as a sound risk management approach, as well as ongoing updates to the Cyber Essentials control themes, such as patching.

This scheme offers the right balance between providing additional assurance of an organisation's commitment to implementing cyber security to third parties, and retaining a simple and low cost mechanism for doing so.

Background

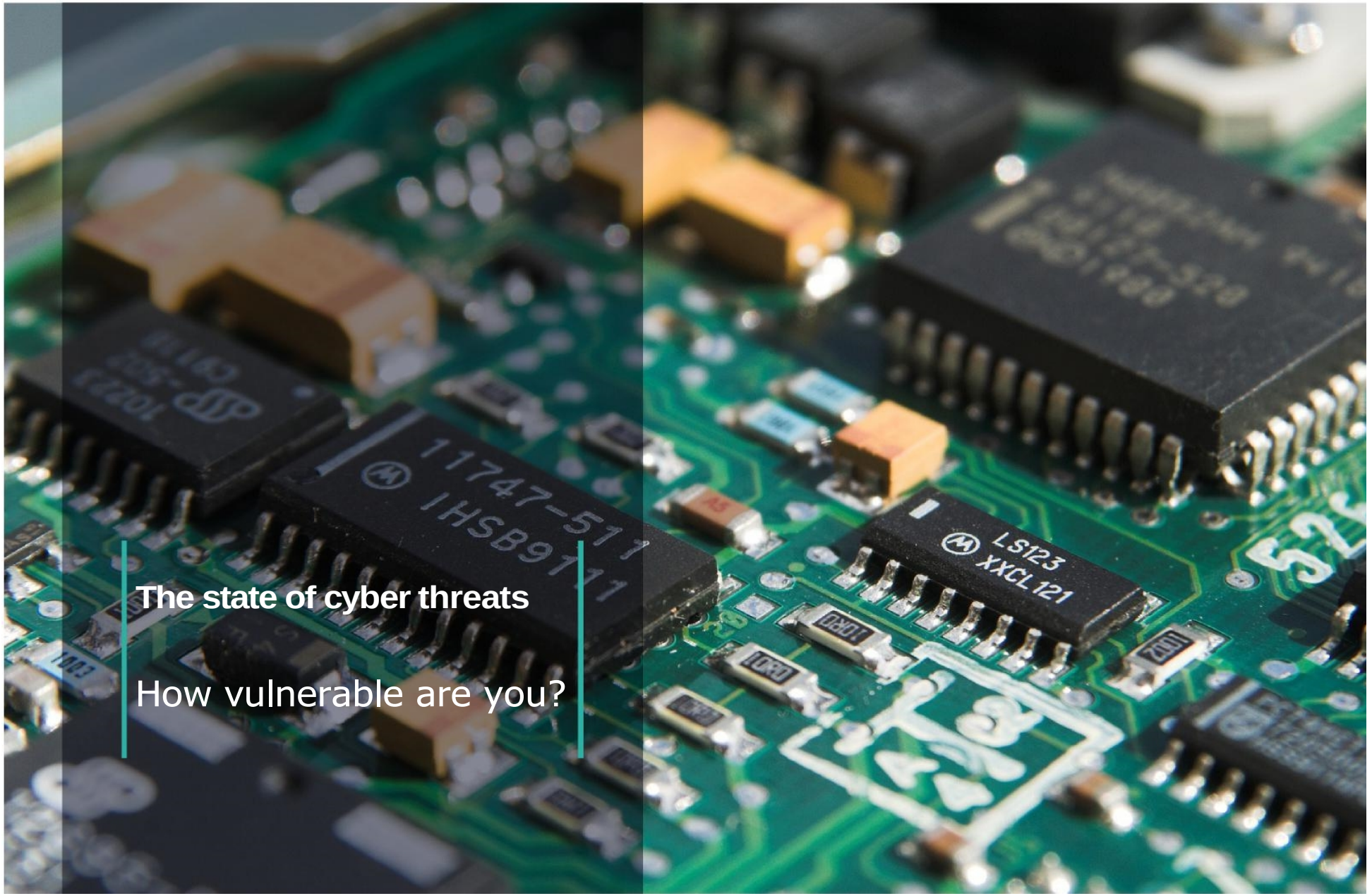
In 2012 the UK government launched its 10 Steps to Cyber Security and then in 2013 published Small businesses: what you need to know about cyber security, which encouraged organisations to consider whether they were managing their cyber risks. The government emphasised the need for company boards and senior executives to take ownership of these risks and enshrine them within their overall corporate risk management regime.

These initiatives continued to gain traction. However, government analysis of continuing attacks and feedback from industry vulnerability testers identified that a number of security controls were not being applied, leaving organisations vulnerable to threat actors with low levels of technical capability.

The government viewed the adoption of an organisational standard for cyber security as the next stage after the 10 Steps to Cyber Security guidance. This was in order to allow organisations, and their customers and partners, to have greater confidence in their ability to reduce the risk posed by threat actors with low technical capability.

Following the call for evidence on a preferred organisational standard in cyber security by the government and industry, the Cyber Essentials scheme was formalised in November 2013.

So why should you achieve Cyber Essentials certification?


The state of cyber threats
How vulnerable are you?

The top 10 common external vulnerabilities account for nearly 52% of all vulnerabilities (2016 NTT Group Global Threat Intelligence Report).

Network outages that are caused by security breaches can often have a long-lasting impact. 45% of such outages last up to 8 hours (Cisco 2017 Annual Cybersecurity Report).

44% of security operations managers see more than 5,000 security alerts per day (Cisco 2017 Annual Cybersecurity Report).

85% of organisations have suffered phishing attacks. (Wombat Security, 2016 State of the Phish).

49% of security professionals said their organisations have had to manage public scrutiny following a security breach (Cisco 2017 Annual Cybersecurity Report).

Half of investigated alerts are deemed legitimate and less than half (46%) of legitimate alerts are remediated (Cisco 2017 Annual Cybersecurity Report).

74% of applications have at least one vulnerability from the OWASP Top 10 (2016 NTT Group Global Threat Intelligence Report).

Nearly a quarter of the organisations that have suffered an attack lost business opportunities. 4 out of 10 said those losses were substantial (Cisco 2017 Annual Cybersecurity Report).

Something as simple as timely patching could block 78% of internal vulnerabilities (2016 NTT Group Global Threat Intelligence Report).

77% of organisations are unprepared for a cyber attack and have no formal plan to respond to incidents (2016 NTT Group Global Threat Intelligence Report).

The business benefits of Cyber Essentials

The benefits of achieving Cyber Essentials certification

The Cyber Essentials scheme provides five security controls, that, according to the UK government, could prevent "around 80% of cyber attacks".

Whether or not you achieve certification to the scheme, these controls provide the basic level of protection that you need to implement in your organisation to protect it from the vast majority of cyber attacks, allowing you to focus instead on your core business objectives.

Properly implemented cyber security has the additional advantage of driving business efficiency throughout the organisation, saving money and improving productivity.

Cyber Essentials certification can also reduce insurance premiums. A government report in March 2015 (UK cyber security: the role of insurance in managing and mitigating the risk) found that the majority of insurers believe "that Cyber Essentials would provide a valuable signal of reduced risk when underwriting cyber insurance for SMEs, allowing them to use a reduced question set and informing their decisions to underwrite", and that "participating insurers operating in the SME insurance sector have agreed to build reference to the Cyber Essentials standard into their cyber insurance applications, and will look to simplify the application where accreditation has been achieved by the applicant".

Protected against approximately 80% of cyber attacks

Implementing the five controls correctly will help you protect your organisation.

Demonstrate security and help secure the supply chain

Achieving Cyber Essentials certification will help you demonstrate your commitment to protecting both your own data and that of your customers and suppliers.

Increase chances of securing business

Cyber Essentials certification will help boost your reputation and give you a better chance of winning contracts.

Drive business efficiency

You will be able to focus on your core business objectives knowing that you are protected from the vast majority of common cyber attacks.

Work with the UK government and MoD

Cyber Essentials will give you the opportunity to work with the UK government and Cyber Essentials Plus will give you the opportunity to work with the Ministry of Defence.

Potentially reduce cyber insurance premiums

Cyber insurance agencies look more favourably on organisations that have acheived Cyber Essentials certification.

How we certify organisations to the CREST-accredited Cyber Essentials and Cyber Essentials Plus schemes

By partnering with IT Governance, a CREST-accredited certification body, we are able to offer you the benefit of an the additional level of independent verification of your cyber security status provided by an external vulnerability scan.

Although non-CREST-accredited certification options exist, none of them offer the same level of independent verification and stakeholder assurance that the CREST-accredited option does.

Hundreds of organisations have certified to the CREST-accredited version of the scheme, with many more achieving certification every day. These organisations have helped boost their competitiveness and are already seeing the benefits of doing so.

SCOPE

The certification can apply to the whole of an organisation's enterprise IT or to a subset of the organisation. The scope needs to be clearly defined before the certification process can get underway. For Cyber Essentials Plus, the scope must also be declared at the beginning of the process.

WHAT IS IN SCOPE AND WHAT IS NOT?

The Cyber Essentials scheme provides protection mainly where IT systems are based on commercial off-the-shelf (COTS) products, rather than large, heavily customised, complex solutions.

The systems that fall under the scope of Cyber Essentials include Internet-connected end-user devices (desktop PCs, laptops, tablets and smartphones) and Internet-connected systems (e.g. email, web and application servers).

In defining the scope, the organisation seeking certification will need to consider the role of service providers who, depending on the delivery of services, may be in scope. The important consideration is whether the organisation or the supplier retains responsibility for the relevant set of controls.

Organisations that use Infrastructure as a Service (IaaS) from a Cloud service provider, and have responsibility for any of the five control sets, will be required to include the service as part of the scope. In the case of Software as a Service (SaaS), where the organisation does not have responsibility for the controls, the service will be out of scope.

Cyber Essentials is not intended for use with bespoke IT systems, such as those found in manufacturing, industrial control systems, online retail and other environments.

Examples of these types of systems are: supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLC), point of sales (POS), PIN entry devices (PED) and e-commerce applications.

SELF-ASSESSMENT QUESTIONNAIRE

Once the organisation has determined the scope, the next step in certification to Cyber Essentials is to complete a self-assessment questionnaire (SAQ). When the SAQ is completed, IT Governance will assess whether it has sufficient confidence that the controls have been effectively implemented.

WHAT ARE THE FIVE CONTROLS?

Secure configuration – makes sure systems are configured in the most secure way for the needs of the organisation.

Boundary firewalls and Internet gateways - these are designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.

Access control – makes sure only those who should have access to systems have access and at the appropriate level.

Patch management – makes sure the latest supported version of applications are used and all the necessary patches supplied by the vendor have been applied.

Malware protection – makes sure virus and malware protection is installed and is it up to date.

CYBER ESSENTIALS

EXTERNAL VULNERABILITY SCAN

Our CREST-accredited certification body will review the questionnaire and conduct an external vulnerability scan of the Internet-facing networks and applications. This scan is used to verify that there are no obvious vulnerabilities present.

WHAT IS REQUIRED?

The aim of the testing is to identify vulnerabilities within an organisation's Internet-facing infrastructure and user workstations that could be exploited by attackers with a low level of skill.

An external full Transmission Control Protocol (TCP) port scan, top User Datagram Protocol (UDP) service scan and a vulnerability scan are required for the stated IP range. A basic web application scan is also required to identify common vulnerabilities.

CYBER ESSENTIALS PLUS

INTERNAL VULNERABILITY SCAN AND ON-SITE ASSESSMENT

Organisations seeking certification to Cyber Essentials Plus will be required to go through the verified self-assessment tests described above, in addition to a series of internal vulnerability tests of the system(s) in scope.

WHAT IS REQUIRED?

The tests required for this stage can be described as an authenticated internal scan and a test of the security and anti-malware configuration of each device type/ build. The internal scan checks patch levels and system configuration, and the security and anti-malware test maskes sure the organisation's systems are resistant to malicious email attachments and web-downloadable binaries.

Tests on inbound email binaries, and payloads, inbound emails containing URLs linking to binaries and browser exploitation payloads are required for the Cyber Essentials Plus scheme. An authenticated vulnerability and patch verification scan is also required.


Why we work with
IT Governance?

Why has Our IT Department partnered with IT Governance to deliver Cyber Essentials and Cyber Essentials Plus certification?

This partnership allows us to help you conduct the entire certification process online through the IT Governance Cyber Essentials portal, without you requiring any expert cyber security knowledge.

We get access to all of the tools and resources needed to help you achieve CREST-accredited certification at both levels of the Cyber Essentials scheme.

As a CREST-accredited penetration testing company, IT Governance can deliver all of the technical tests and assessments.

Through our partnership with a CREST-accredited certification body like IT Governance, you will benefit from the added level of independent verification of your cyber security status provided by an external vulnerability scan.

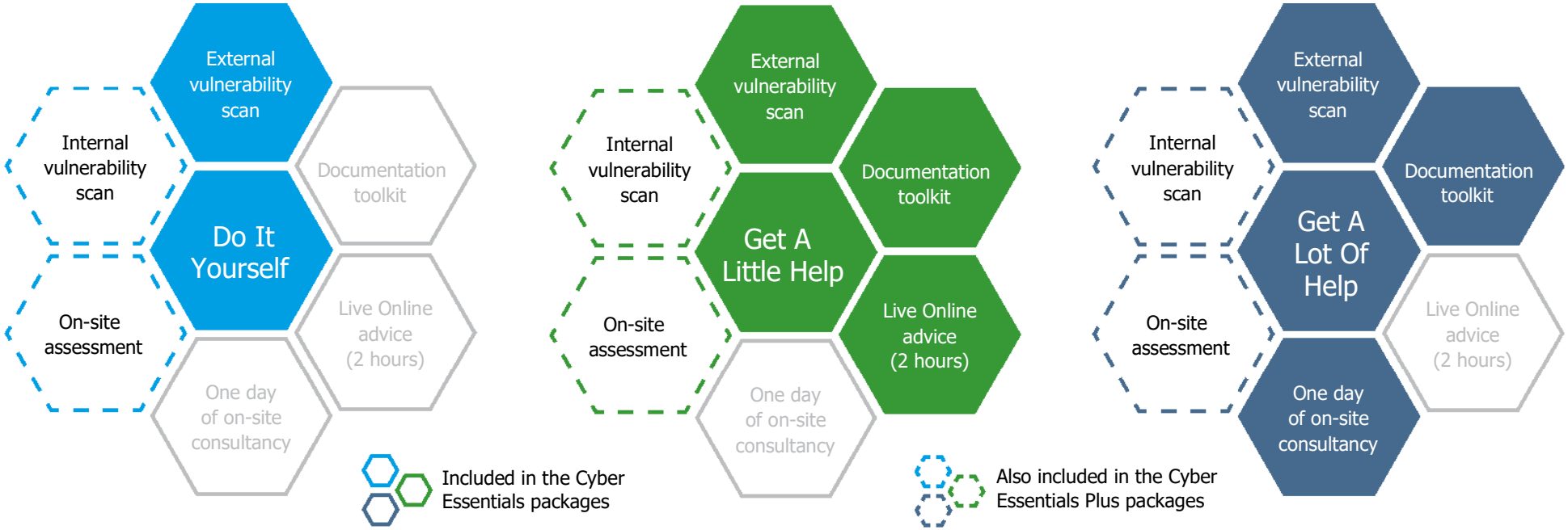
We can offer six packaged solutions to support certification to either Cyber Essentials or Cyber Essentials Plus at a pace and for a budget that suits you.

Having led ISO 27001 implementations since the inception of the standard, our partnership gives you access to the knowledge and insight to help you take the next steps beyond Cyber Essentials.

Some of IT Governance's Cyber Essentials clients include companies such as:


Our solutions
Designed to help all
levels of experience

Our packaged solutions can help you achieve certification to either Cyber Essentials or Cyber Essentials Plus at a pace and for a budget that suits you.



External vulnerability scan

All of our Cyber Essential packages include an external vulnerability scan. This independently verifies the security status of each company that undergoes Cyber Essentials certification through us.

Documentation toolkit

Includes all of the necessary customisable policies and procedures to meet the Cyber Essentials requirements. The templates include guidance on correctly implementing and maintaining your cyber security controls.

Live Online advice (2 hours)

If you need guidance or just peace of mind on any part of the Cyber Essentials certification process, then our Live Online consultancy is perfect for you.

One day of on-site consultancy

Conducted by an expert cyber security practitioner. They will provide guidance on completing the self-assessment questionnaire and how to implement the five controls required by the scheme, and will help define the scope for certification.

Internal vulnerability scan

Involves a scan of your in-scope internal network, with a focus on workstations and mobile devices. It aims to find out whether the Cyber Essentials controls have been properly implemented and to check that known vulnerabilities have been addressed.

On-site assessment

We will visit your office(s) and thoroughly check whether the solutions you have put in place comply with the control requirements.

IT Governance's credentials

- IT Governance is a global leader in information and cyber security management systems expertise.
- IT Governance is a CREST member company and has been verified as meeting the high standards mandated by CREST.
- Their expertise in standards such as the Payment Card Industry Data Security Standard (PCI DSS), ISO 27001, the General Data Protection regulation (GDPR) and ISO 9001 means we can offer an integrated approach to compliance.
- They provide independent and unbiased advice – they are not affiliated with any software or hardware solution.
- IT Governance is an IBITGQ Accredited Training Organisation (ATO), and an official publisher of the IBITGQ study guides and courseware.
- Their cost-effective and customised advisory services provide a tailored route to achieving improved cyber security, scalable to your budget and needs.

Some of IT Governance's other customers:

BGD IT Department
Montague Place 13
BN11 3BG Worthing
West Sussex

t: +44 (0) 777 8429591
e: info@businessgodigital.uk
w: www.businessgodigital.uk