Cyber Testing
Playbook

Protect • Comply • Thrive

governance™

Better Security, Better Value

Today, most buyers see no real difference between cyber testing vendor propositions.

Information technology is driving business efficiency and productivity, and the digital economy is thriving as growing numbers of organisations are benefiting from the opportunities the Internet brings. However, cyber crime is increasingly easy to perpetrate, and the threats the modern organisation faces are intensifying.

According to a recent survey conducted by Opinium for internet service provider Beaming, 52% of UK businesses – some 2.9 million firms – fell victim to some form of cyber crime in 2016, at a total cost of £29.1 billion (Beaming, Cyber Report 2016: UK businesses targeted 230,000 times each by cybercriminals).

It's not just big businesses that are at risk, either: 2016 research from the Federation of Small Businesses found that 66% of small businesses have been a victim of cyber crime (FSB, Cyber Resilience: How to protect small firms in the digital economy).

If this seems surprising, remember that every organisation holds data – such as employee payroll details, proprietary data or client information – that has a value to someone. Moreover, many attacks on larger companies have been perpetrated as a direct result of an exploit on smaller third-party suppliers.

The recent surge in cyber attacks has attracted a great deal of media attention and cyber security is, at last, a mainstream concern. This, combined with the fact that the EU General Data Protection Regulation (GDPR) will bring huge administrative fines for breaches when it is enforced from May 2018, has prompted companies of all sizes to take a hard look at their information security controls.

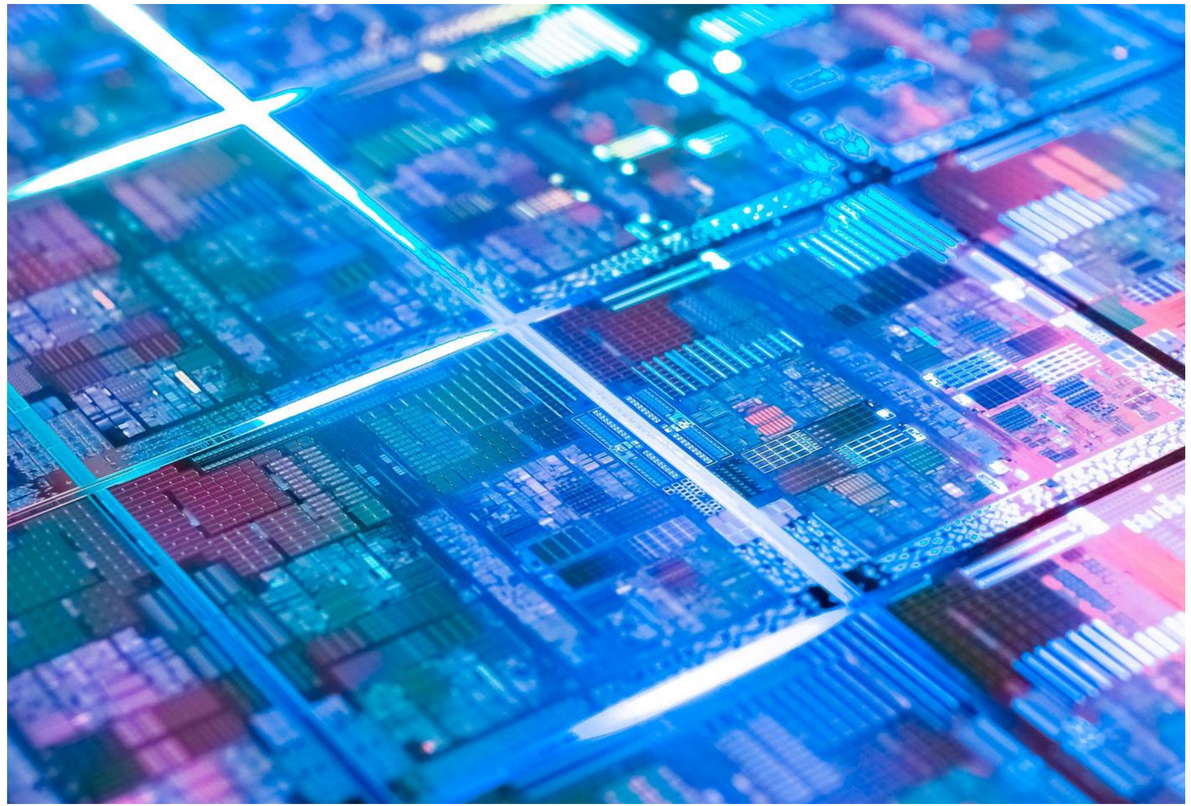
The majority of cyber crimes are opportunistic. Automated attacks exploit known vulnerabilities in unpatched software, untrained staff are lured into opening malicious attachments or clicking malicious links in phishing emails, and drive-by attacks install malware on users' machines. This is why it is so important to secure your network and applications from attackers, and to train all staff to be aware of their responsibilities. Finding the internal resource to do so, however, is no mean feat.

The well-documented cyber security skills gap shows no sign of closing: as demand for cyber security specialists has increased, they have become even more difficult to hire. There were 1 million cyber security job openings in 2016, and that number is expected to reach 1.5 million by 2019 (UK House of Lords Digital Skills Committee).

Perhaps unsurprisingly, this skills shortage is why Cybersecurity Ventures predicts global spending on cyber security products and services will exceed $1 trillion over the next five years (Cybersecurity Ventures, 2016 Cybercrime Report). However, many buyers find the information security marketplace overcrowded and confusing, with seemingly little or no difference between vendor propositions.

So what sets a good cyber testing company apart from the rest of the field?

Keep reading



If a business is connected to the internet in any way, it needs to achieve some level of cyber security. Many buyers find the marketplace over-crowded and confusing, with seemingly little or no difference between cyber testing vendor propositions.

So what sets a good cyber testing company apart from the rest of the field?

The most important factors to consider when evaluating a cyber testing company are:

Whether it has proven expertise in ethical hacking and data protection

Top vendors have robust threat assessment methodologies and tests that validate the risks posed by specific security vulnerabilities or flawed processes, so that you can prioritise remediation. Such companies can demonstrate their ethical hacking capabilities with documentation of previous exercises. There is a reason these companies have good reputations: they can back up their claims quickly and efficiently.

Whether it has the ability to adapt to emerging threats and compliance requirements

Top vendors have the flexibility to adapt to the evolving threat landscape. Cyber threats take a variety of forms and can originate from both external and internal actors. Cyber testing firms need to offer a range of disciplines to cover all threat vectors to provide protection from the inside as well as from the outside. In addition, they need to be able to offer practical experience of having put in place appropriate cyber security frameworks.

Whether it can provide assurance that work will be conducted by qualified individuals

Vendors should be held to standards of excellence. Testers should have practical experience and professional certifications or credentials to certify their competency. Accreditations, such as CREST, provide organisations wishing to buy penetration testing services with confidence that the work will be carried out by qualified individuals with up-to-date knowledge, skill and knowledge of the latest vulnerabilities and techniques used by real attackers.

The State of Cyber Threats

Network outages that are caused by security breaches can often have a long-lasting impact. 45% of such outages last from 1 to 8 hours (Cisco 2017 Annual Cyber Security Report).

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

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

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

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

Organisations can investigate only 56% of the security alerts they receive on a given day (Cisco 2017 Annual Cyber Security Report).

Only 42% of respondents believe their company has the tools to mitigate external threats. (Ponemon Institute, Security Beyond the Traditional Perimeter).

53% of organisations experience delays as long as 6 months when seeking qualified security candidates (ISACA and RSA Conference, State of Cybersecurity: Implications for 2015).

84% of organisations believe that less than half of applicants for open security jobs are qualified (ISACA and RSA Conference, State of Cybersecurity: Implications for 2015).

Most organisations rely on third-party vendors for at least 20% of their security measures (Cisco 2017 Annual Cyber Security Report).

There is a severe shortage of cyber security talent globally: there were 1 million cyber security job openings in 2016, and this number is expected to rise to 1.5 million by 2019 (UK House of Lords Digital Skills Committee).

50% of companies now believe security training and awareness for both new and current employees is a priority (Dell's Protecting the organization against the unknown – A new generation of threats).

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

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

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

27% of connected third-party cloud applications introduced by employees into enterprise environments in 2016 posed a high security risk (CloudLock Q2 2016 Cloud Cybersecurity Report: The Explosion of Apps: 27% are Risky).

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

A cyber security health check **How strong are your foundations?**

The following are typical signs that your cyber security foundations are not as strong as they should be.

- Your organisation lacks a risk-based cyber security management system.
- There has been no assessment of your organisation's vulnerability to attack or the value and exploitability of critical assets.
- Your organisation has yet to implement your cyber security policy as an issue because your staff are not sufficiently aware of or engaged with it.
- You struggle to understand how compliance rules fit or need to be integrated into your wider cyber security plans, policies and defences.
- Your organisation lacks sufficient controls to set and monitor user access levels to prevent privilege abuse and the potential loss of data.
- You lack a recovery plan, even though having one is critical to your response time and for the resumption of business activities.
- There is inadequate linkage between security testing and requirements such as PCI DSS and GDPR.
- Your organisation currently lacks the capability to detect external cyber threats.
- You lack the ability to analyse data to get a clear assessment of the vulnerabilities and the levels of risk they present to your organisation.
- Critical employees are not qualified or capable of acting in the organisation's best interest in the event of a cyber breach.
- Your organisational mindset is focused more upon investigating individual incidents than investing in prevention activities.
- You lack senior management support to ensure an adequate level of protection from common vulnerabilities and attacks.

These are not uncommon issues. Most CIOs and CISOs will admit they encounter these warning signs from time to time, even though most will have spent significant time and resource on strengthening their company's defences against cyber security risks.

So what are the main causes of these issues?

Why this is happening

The face of cyber security is changing constantly. Here are ten cyber predictions and trends that organisations need to be aware of when preparing their cyber security defences.

Organisations will have to automate to keep up with criminals

Attackers' capability to write bespoke, targeted code will continue to improve faster than the defenders' ability to prevent or counter attacks, and there will continue to be a shortage of people with the right expertise to counter this ever-growing threat. As well as investing in skills and recruitment, the solution lies in automating manual processes and implementing system analytics.

Breaches will get more complicated and harder to beat

Ransomware will remain a significant threat. Ransomware-as-a-service, custom ransomware for sale in dark markets and creative derivatives from open-source ransomware code will keep the security industry busy. Ransomware's impact across all sectors and geographies will force the security industry to take decisive actions. Initiatives like the No More Ransom! collaboration, the development and release of anti-ransomware technologies, and continued law enforcement actions will reduce the volume and effectiveness of ransomware attacks.

Companies will need to get firm on bring-your-own-device (BYOD) policies

Employees will continue to disregard corporate protocols and download malware-laden mobile apps from unauthorised app stores onto the devices they use to connect to corporate networks. Even when they follow recommended practices, there's still a risk; reputable stores have sometimes been fooled by rogue developers who create malicious development environments designed to hide malware in apps that appear to be safe.

There will be more security available in the Cloud

One thing is certain: the Cloud is not going away, and more enterprises will migrate key services to the Cloud and start designing their future intelligent infrastructures on Cloud-based models.

An attack that disrupts or takes down a major Cloud provider would affect all of their customers' businesses. Because of the potential scale of impact, motives will be difficult to determine, but will vary from causing general chaos to targeting a specific competitor or organisation.

Organisations handling EU residents' data will be concerned about the General Data Protection Regulation (GDPR)

The GDPR, which will apply from May 2018, helps to protect EU residents' privacy and personal data.

Firms that do not comply with the GDPR could face hefty fines of up to €20 million or 4% of their annual global turnover (whichever is higher). With the enforcement deadline so near, expect the GDPR compliance focus to shift from legal to chief information security officers.

The Internet of Things (IoT) will have repercussions across the business spectrum

The IoT merges the physical and online worlds, opening up a host of new opportunities and challenges for companies, governments and consumers.

When businesses provide suppliers with access to IoT devices on their networks, they risk opening the door to hackers. Once inside, hackers can take over connected devices and use them as part of a bigger hack or distributed denial-of-service attack.

Collaboration will be the solution for just about every aspect of supply-chain management except one: cyber security

The very nature of global supply chains demands that companies exchange sensitive information with multiple partners, some of them several tiers removed from the provider. Their ability to protect data can be highly variable.

To be safe, companies must continually ensure confidence in third parties' data safeguards, security policies and procedures, and determine whether their security posture is sufficient to respond to a data breach or cyber attack.

Organisations will need to focus on data integrity

Attackers will start to set their sights on compromising data integrity. This type of attack, in comparison with a straightforward theft of data, will serve to cause long-term reputational damage to individuals or groups by getting people to question the integrity of the data.

Organisations must get serious about monitoring and managing third-party risk

The emphasis will likely shift from snapshot-in-time monitoring to continuous monitoring. The increased regulatory focus on vendor risk, coupled with the GDPR, means that firms won't be able to continue outsourcing their security risk to third parties, and will require significant internalisation of threat detection services.

The cyber security skills shortage will hold steady

Cyber security has been identified as the number one "problematic shortage" area across all of IT for the past six years in a row. In 2017, 45% of organisations say they have a "problematic shortage" of cyber security skills. Furthermore, when Information Systems Security Association (ISSA) members were asked to identify the impact of the cyber security skills shortage on their organisation, 35% said a lack of cyber security skills has led to an inability to use some security technologies to their full potential (Enterprise Strategy Group, 2016 IT Spending Intentions Survey).

What should you be looking for from your suppliers?

You should consider several factors when deciding to hire a cyber testing consulting partner to make sure you choose one that has the necessary tools and offers the right mix of know-how and experience to provide holistic, cost-effective and compliant security solutions. Such factors include the following:

1. Primary focus on cyber security

A good vendor won't rely solely on technological solutions but will take a holistic approach to protecting your organisation.

2. Accredited penetration testers

You should use a vendor with a CREST-certified penetration testing team or testers accredited to equivalent CREST levels. You can also find certified companies through the CREST Approved members list of companies.

3. Service breadth and experience

To deliver the right solution for you rather than a one-size-fits-all approach, your chosen vendor needs to have experience across a diverse set of disciplines and customers. This enables you to leverage the experiences and lessons of other firms.

4. Long-term-relationship focus

A good vendor will invest the time to learn about your organisation's needs, help you to reduce costs and help to redefine the scope of your cyber security plan over time as your requirements evolve.

5. 100% vendor agnostic

Your chosen vendor should not be affiliated with any hardware and/or software solution. If they're not vendor-agnostic, there's no guarantee of independent, unbiased advice.

6. Compliance experience

A good partner will be able to structure a framework to achieve all of your compliance, legal and stakeholder requirements, which should be agreed from the outset as part of your testing programme.

7. Specialised training

Helping you to improve your cyber security posture may require training, whether of your entire staff, security team or executive leadership. If a vendor is proficient in the technical aspects of security, but cannot offer training as well, their utility is limited.

How we take action

Cyber security comes down to preventing breaches, detecting the ones that happen and then responding intelligently to minimise their impact.

As attacks become easier to perpetrate, and the potential damage caused by cyber attacks becomes increasingly disruptive, organisations must improve their cyber defences.

The traditional approach to IT security, which focuses on the technological aspects, is only one part of the solution. In order to protect their business assets in cyberspace – including reputation, IP, employees and customers – organisations need to take an integrated and intelligence-led approach to cyber security that also considers processes and people.

IT Governance is the world's only Governance, Risk and Compliance one-stop-shop with a range of products and solutions that can be tailored to help organisations of any size achieve their cyber security aims at an affordable cost.

IT HEALTH CHECK

Do you have an overall view of how effective your security plan is? Are the right IT security controls in place to protect the information that is critical to your business? Performing an IT health check provides senior management with an independent and holistic view of IT security and challenges, and recommendations for improvements.

HOW?

We can undertake an analysis of your chosen systems and network to identify any vulnerabilities that may compromise the confidentiality, integrity or availability of information held.

CYBER ESSENTIALS CONSULTANCY AND CERTIFICATION

The government requires all suppliers bidding for contracts that include the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme. Certification also puts you in a strong position to gain new business, both in the public and private sectors.

HOW?

We can help you achieve certification to either Cyber Essentials or Cyber Essentials Plus. Our CE portal enables companies to follow a convenient do-it-yourself approach, including managing and tracking the certification process.

ADVANCED PENETRATION TESTING

Most organisations are the target of indiscriminate attacks and they need an appropriate level of penetration testing to ensure their defences are adequate. Instead of automatically generated reports from tools that offer generic remediation tips, you need advice from experts who can rank and rate your vulnerabilities so that you can plan the remediation actions in accordance with the risk and your budget.

HOW?

We can test your defences with our penetration testing services. By simulating an attack, we can detect your business-critical vulnerabilities and work with you to protect your systems.

CONFORM TO THE PCI DSS

The PCI DSS applies to all organisations worldwide that transmit, process or store payment card data. With rules governing everything from data encryption to network segmentation, compliance with the PCI DSS requirements can be difficult to achieve and maintain. What matters to all organisations is effective, timely compliance with the PCI DSS delivered within an acceptable budget.

HOW?

We cover the entire range of payment card compliance services. As an authorised QSA company, we can assess your needs, carefully explain the PCI compliance requirements relevant to you, and provide solutions that will suit your budget.

PROTECT YOUR DATA

Penetration testing is an essential component of any ISO 27001-compliant information security management system (ISMS), from initial development through to ongoing maintenance and continual improvement. A penetration test is the best method for identifying vulnerabilities in systems, infrastructure and web applications.

HOW?

We can conduct a penetration test on the assets that are to be included in the scope of your ISMS.

We can also help you implement the ISO27001 ensuring that all the requirements of the Standard are met with minimal disruption to your business.

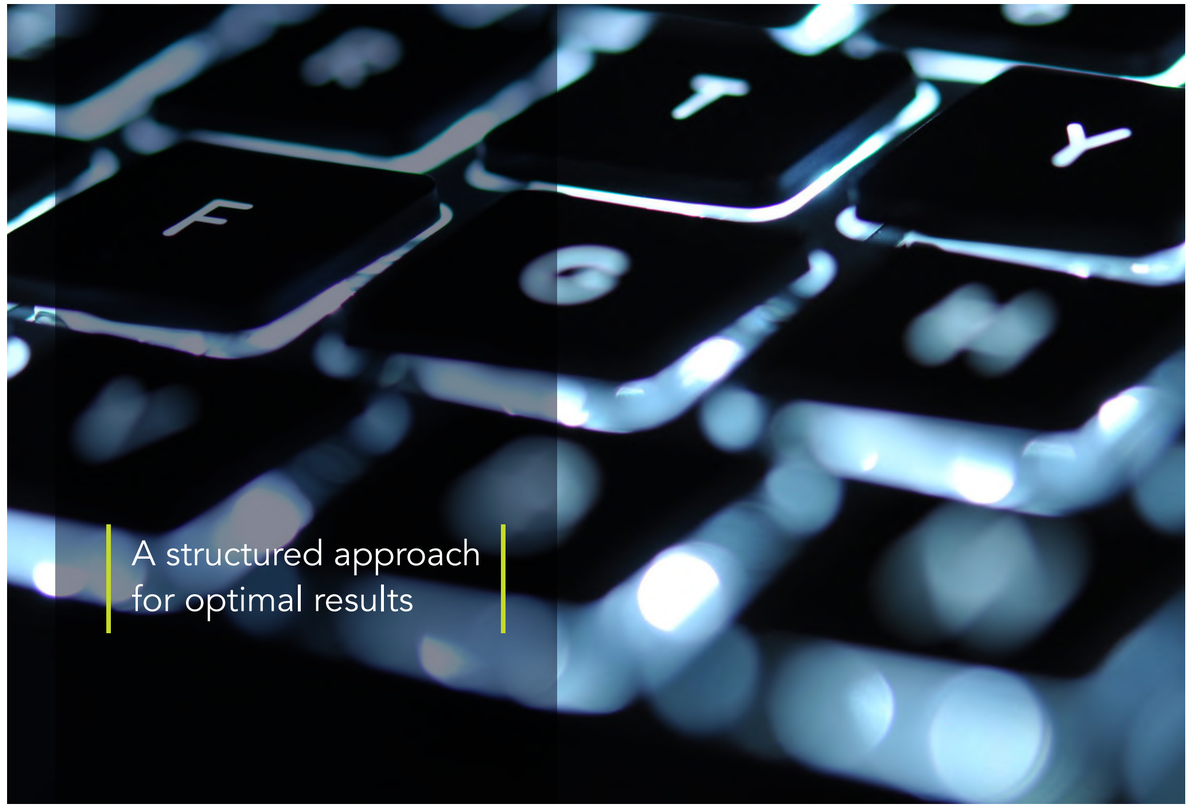
TRAINING AND ON-GOING SUPPORT

In the context of cyber security, the adage that you are only as strong as your weakest link is particularly pertinent; it is important to consider your cyber security strategy as a whole, and that means not just managing your technology but also your people.

HOW?

We offer training courses (both classroom and in-house) for all staff, from basic foundation level through to advanced courses.

With our Live Online consultancy service, you can purchase consultancy support by the hour, so you can get the support you need quickly.



A structured approach for optimal results

Our structured and proven approach provides tangible results at a competitive price, and has proved to be of particular interest to small and medium-sized enterprises.

PROTECT

Assess how to strengthen your defences against a cyber attack

- Define your overall risk appetite
- Identify the most important information and applications where they reside and who has or needs access
- Assess the threat landscape and highlight your real exposure

PREVENT

Understand current and future threats and the actions needed to prevent them

- Develop a security strategy focused on organisational goals and protecting high-value data
- Intelligently prioritise remediation, apply security patches and allocate security resources more effectively
- Establish and rationalise access control

PERFORM

- Make security everyone's business
- Broaden the programme to adopt enterprise-wide information risk management concepts
- Set metrics that influence business performance

PREPARE

Find out how to mitigate the impact of a security breach

- Allow good security to drive compliance, not vice versa
- Accept manageable risks that improve performance
- Spend wisely on controls and technology

Our services

Penetration testing

At IT Governance, we offer two levels of penetration test to meet your budget and technical requirements. In most cases, we recommend a level 1 penetration test, which is a faster and more cost-effective solution at a fixed price, and will identify exploitable vulnerabilities and remediation solutions. A level 2 tests offers a more complete test that aims to identify methods a criminal hacker could use to gain control of your system.

As a CREST member company, IT Governance has been verified as meeting the rigorous standards mandated by CREST. We are able to offer black-box ('blind') tests, white-box ('full disclosure') tests, or something in between, tailored to your requirements. We can extend this test to web applications and WLANs, with savings available for annual contracts.

Network pen testing

Web application pen testing

Employee phishing vulnerability

Assessments for the Cyber Essentials Scheme

Our CREST-approved technical services team will conduct vulnerability analysis and verification in line with the Cyber Essentials test specification. Our CE portal is the leading CREST-accredited route to CE certification.

IT health checks

We can undertake an analysis of your chosen systems and network to identify any vulnerabilities that may compromise the confidentiality, integrity or availability of the information you hold. We will help you scope your IT health check to ensure it is a worthwhile exercise and provides you with the correct level of assurance.

PCI DSS consultancy service

Our status as an approved Qualified Security Assessor (QSA) company underpins our range of PCI DSS consultancy services, which include scoping, gap analysis, remediation support and audit. We offer the full range of PCI QSA services.

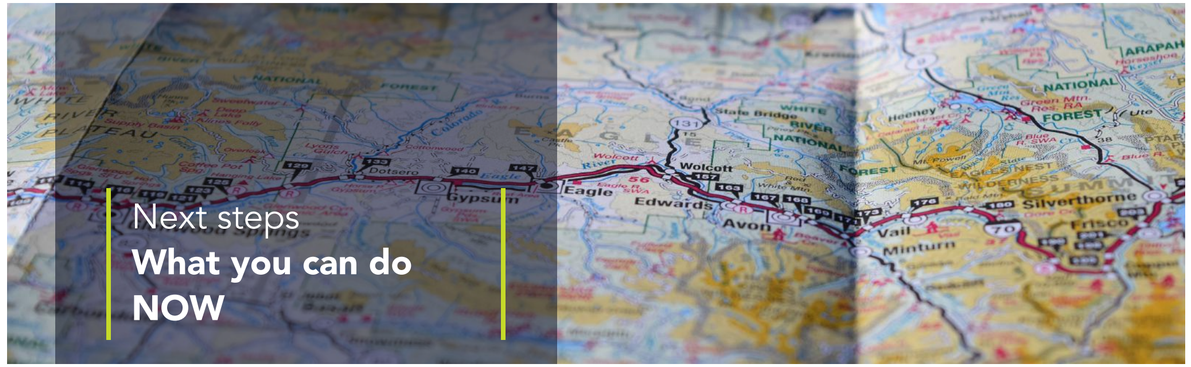
Our role is to ensure that an organisation is fully compliant with the requirements as specified in the PCI DSS. All QSA companies must comply with and adhere to a number of rigorous business and technical requirements as specified by the Payment Card Industry Security Standards Council (PCI SSC).

Training and knowledge transfer

We offer training courses (both classroom and in-house) for all staff, from basic foundation level through to advanced courses for IT practitioners and lead implementers seeking compliance with or certification to various standards, including ISO 27001 and the PCI DSS, as well as professional certifications like the CEH and CISSP.

Our unique and unrivalled training portfolio is designed to ensure organisational efficiency and compliance, as well as to support your career development.

Our courses lead to qualifications awarded by APMG, EXIN, BCS, (ISC)2®, ISACA® and the International Board for IT Governance Qualifications (IBITGQ).



Next steps
What you can do NOW

We have a team of account managers and security consultants available to discuss your cyber testing challenges. **Whether you have never undertaken a security test or already have a mature security programme in place, whether you are at the start of your compliance journey or looking to switch suppliers, we can help.**

Here's what you can do next:

Use the cyber security health check in this playbook as a starting point for a conversation:

- Identify the main challenges you're facing.
- We'll discuss possible root causes and gaps in your security – and how to fix them.

Or simply call
00 800 48 484 484
to speak to a security specialist and get more information.

Our 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.
- Our expertise in standards such as the PCI DSS, ISO 27001, the GDPR and ISO 9001 means we can offer an integrated approach to compliance.
- We provide independent and unbiased advice – we 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.
- Our cost-effective and customised advisory services provide a tailored route to achieving improved cyber security, scalable to your budget and needs.

Our customers

IT Governance Ltd
Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA, United Kingdom

t: 00 800 48 484 484
e: servicecentre@itgovernance.eu
w: www.itgovernance.eu

@ITGovernanceEU /it-governance /ITGovernanceEU