Data Sheet
The PCI DSS

Protect profits by managing payment card risk

IT Governance is uniquely qualified to provide Payment Card Industry (PCI) services. Our leadership in cyber security and technical services enables us to offer unique and efficient approaches providing advice about meeting increasingly tougher requirements, while still serving as a business partner to improve your long-term security posture and keep costs under control.

Did you know?

66% of customers say they would be unlikely to do business with an organisation that experienced a breach where their financial and sensitive information was stolen.

Verizon 2017 Payment Security Report

Authorised QSA company

As an authorised QSA, we can advise on challenging aspects of the PCI DSS. Our cost-effective and customised advisory services provide a tailored route to PCI compliance, scalable to your budget and need.

Focused on improving security, not just compliance

Our approach to helping clients is to help strengthen their security posture rather than offering an audit based service. We can offer an integrated approach to PCI DSS compliance due to our expertise in other internationally adopted standards, such as ISO 27001 and ISO 9001.

Minimise business disruption and costs

Our experts can help build the PCI requirements into everyday business processes to ensure continual compliance and ease the burden at annual audits. We work with our customers to assure PCI compliance while minimising business disruption, keeping costs down and ensuring improved customer engagement.

it governance™

Protect • Comply • Thrive

Who needs to be compliant?

Merchants

Brick-and-mortar, mail/telephone order, e-commerce and virtually anyone that processes payment cards across all industries

Service providers

Payment service providers, managed service providers, web hosting providers, transaction processors, data centres and independent sales organisations

Financial institutions

Banks, finance providers, brokers and insurance companies

PCI validation requirements

The following tables describe the validation requirements for both merchants and service providers from Visa and Mastercard.

🔍 Quarterly ASV scanning

✓ Yearly SAQ

📄 Annual on-site QSA audit

For merchants:

Transactions	Requirements
For organisations processing fewer than 6M Visa or Mastercard transactions annually	🔍 ✓
For organisations processing more than 6M Visa or Mastercard transactions annually	🔍 ✓ 📄

For service providers:

Transactions	Requirements
For organisations processing fewer than 300K Visa or Mastercard transactions annually	🔍 ✓
For organisations processing more than 300K Visa or Mastercard transactions annually	🔍 📄

PCI DSS Consultancy Services

Our PCI QSAs provide experience and practical advice to help you improve your current security programme and meet the requirements of the PCI DSS.

We provide a consultative approach to compliance and will work in partnership with you to identify opportunities to lower cost and reduce complexity. We can provide advice on the use of valid compensating controls, or architect a solution that includes them.

Our QSAs will lead you through the PCI journey and help build requirements into everyday business processes to ensure continual compliance and to ease the burden at annual QSA audits.

Assess your current PCI compliance posture.

A PCI DSS gap analysis is a review of an organisation's cardholder data environment (CDE) against the latest version of the Standard. This service reviews in-scope systems and networks to provide a detailed report about the areas that need attention. The service can help your organisation pass its annual PCI audit, or build a CDE and infrastructure that meet the requirements of the Standard. Our PCI DSS gap analysis helps you use PCI compliance as the starting point for a security strategy.

Achieve and maintain PCI DSS compliance within a timeframe that suits your business.

IT Governance's Payment Card Industry Data Security Standard (PCI DSS) implementation and continual improvement service helps customers by documenting and providing a comprehensive plan for the remediation tasks they need to undertake to fully comply with the relevant PCI DSS requirements.

PCI DSS remediation is an essential phase for organisations wishing to comply with the Standard. Although implementing these changes can be costly both in time and in resources, an expert-driven remediation plan can significantly streamline compliance efforts.

Receive a fully documented Report on Compliance (RoC) that is accepted by your business partners .

A PCI DSS compliance and audit service helps customers establish whether they meet the requirements of the PCI DSS.

A PCI RoC is required by organisations with large transaction volumes and must be conducted by a QSA who will issue a formal report to the Payment Card Industry Security Standards Council (PCI SSC) to confirm if your organisation is in full compliance.

Confirm that the controls required by the PCI DSS are in place and effective.

PCI compliance, especially for Reports on Compliance (ROCs) and some self-assessment questionnaires (SAQs), requires internal and external vulnerability scans, and regular penetration tests. Regular testing is fundamental to ensuring that an organisation is prepared for the full range of attacks that companies face.

Our CREST-accredited penetration testers can assess your data security by applying real-world security testing of the controls you believe are in place and functioning effectively.

Merchants/service providers	**Annual on-site audit**	**SAQ**	**Quarterly* external vulnerability scan (ASV)**	**Quarterly* internal vulnerability scan**	**Annual** penetration test (Level 2)**	**Quarterly wireless network analysis**	**Annual web application vulnerability scan[1]**
			Req. 11.2.2	**Req. 11.2.1**	**Req. 11.3**	**Req. 11.1**	**Req. 11.3.1**
RoC	✓		✓	✓	✓ ++	✓	✓
SAQ D for merchants		✓	✓	✓	✓	✓	✓
SAQ D for service providers		✓	✓	✓	✓ ++	✓	✓
SAQ C		✓	✓	✓	✓ #	✓	
SAQ C-VT		✓			✓ #		
SAQ P2PE-HW		✓					
SAQ B		✓					
SAQ B-IP		✓	✓		✓ #		
SAQ A-EP		✓	✓	✓	✓ +		✓
SAQ A		✓					

* Or after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications or product upgrades).

** Or after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a subnetwork added to the environment, or a web server added to the environment).

# Only required for testing network segmentation if any is present.

+ Only external penetration test required.

++ For service providers, any network segmentation must be tested every six months.

[1] Or after any change to the application. Applicable if developing own applications or using a third-party non-PCI-certified web application.

Build PCI compliance into your cyber security programme

IT Governance's approach uses the PCI DSS as a set of information security controls that can be effectively integrated within a broader cyber security and ISO 27001 management system to achieve greater efficiencies and further reduce risk.

We can also help you develop your GDPR framework in a way that integrates PCI DSS at the same time.

The new EU General Data Protection Regulation (GDPR), which became law on the 21st of April and will become enforced on the 25th of May 2018 will require businesses to take PCI DSS more seriously. The GDPR fines (up to €20,000,000 or 4% of turnover, whichever is the greater) will not only supersede the PCI DSS fines but more importantly the GDPR will enforce public reporting of any PCI DSS breach.

We can help develop a framework that helps achieve compliance with GDPR. The PCI DSS has a set of well-established protocols and methodologies. If these were to be adopted for all personal data, not simply cardholder data, then compliance with GDPR standards can be achieved more easily. This is a significant advantage to those that are currently scoping a project.

Our solutions

We can work with your organisation to implement suitable solutions that will enable you to reduce your risks and ensure compliance with the PCI DSS.

Validation and SAQ support	Our facilitated SAQ service provides a QSA to manage compliance for level 2, 3 and 4 merchants, and level 2 service providers.	We will help you identify the right SAQ to complete and provide the appropriate support and advice to achieve full compliance with the PCI DSS.
PCI gap analysis	A detailed review of your current PCI compliance posture that produces a strategic roadmap to compliance with the Standard.	A PCI DSS gap analysis will help your organisation prepare to pass the annual audit, or to help you build a cardholder data environment and infrastructure.
PCI implementation	We can help manage your team's PCI DSS remediation efforts, delivering cost-effective solutions closely aligned with the target environment and your broader security strategy.	Receive a clear and concise plan to reach full compliance that demonstrates efficient use of budget and resources for executive sponsorship and funding.
Compliance audit and RoC	A PCI DSS audit conducted by an IT Governance QSA provides a thorough assessment of the controls you have implemented and establishes whether they meet the requirements of the Standard.	Obtain a complete review of your cardholder data environment to evidence that your controls are in place and working effectively.
Penetration testing	Meet the penetration testing requirements of the PCI DSS with our comprehensive web application, infrastructure or wireless network penetration tests.	Establishes whether and how a malicious attacker could gain unauthorised access to your systems and determines whether the controls required by the PCI DSS are in place and effective.
Documentation toolkit	For smaller organisations, our documentation toolkit contains all the expert guidance, advice and fully customisable documentation templates you will need to accelerate your PCI DSS project.	Become your own expert with professional guidance to embed the documentation into your organisation quickly and easily by using pre-formatted templates.

Training and awareness

We also offer courses to help raise awareness and train individuals who are involved in PCI DSS implementation, in order to help organisations successfully implement the PCI DSS and ensure year-to-year maintenance of the certification.

PCI DSS Foundation Course

Offers an introduction to the PCI DSS and delivers practical guidance on how it applies to your organisation.

PCI DSS Implementation Course

A two-day course that covers all aspects of implementing a PCI DSS compliance programme.

PCI DSS Online Course, Staff Awareness Edition

Implement a formal security awareness programme to make all personnel aware of the importance of cardholder data security.

Our company

IT Governance is the world's leading global provider of IT governance, risk management and compliance solutions. Our comprehensive range of products and services, combined with flexible and cost-effective delivery options, provide a unique, integrated alternative to the traditional consultancy firm, publishing house, penetration tester or training provider.

Companies that use our PCI DSS products and services:

OLIVER BONAS

Volkswagen

PIZZA PAPA JOHN'S

BETFRED

Our PCI credentials and corporate certificates:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

ACCREDITED IBITGQ Certifying Competence TRAINING ORGANISATION

ISO 27001 CERTIFICATION EUROPE™

ISO 9001 CERTIFICATION EUROPE™

IT Governance Ltd

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

t: +44 (0)333 800 7000
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

/ITGovernanceLtd

/ITGovernanceLtd

/ITGovernanceLtd