Data Sheet
The PCI DSS

Protect profits by managing payment card risk

The Payment Card Industry Data Security Standard (PCI DSS) applies to all organisations that transmit, process or store payment card data. Although the Standard is technically complex to implement, it is based on common information security practices. Broken down into six major security goals with 12 areas of focus, the PCI DSS could impose a possible 288 requirements onto your organisation.

Did you know?

80% of organisations failed their initial PCI compliance assessment in 2014.

71% of organisations fell out of compliance less than a year after being assessed compliant.

Verizon 2015 PCI Compliance Report

Our team of consultants can help you address these challenges:

- 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 that meets the requirements of the Standard. You'll find out where improvements are needed and what steps to take to close the gaps.
- For smaller organisations, our PCI DSS Documentation Toolkit contains all the expert guidance, advice and fully customisable documentation templates you will need to accelerate your PCI DSS project.
- For larger organisations, our team can deliver a PCI QSA audit and the Report on Compliance (RoC) to attest that your organisation is in full compliance with the PCI DSS.

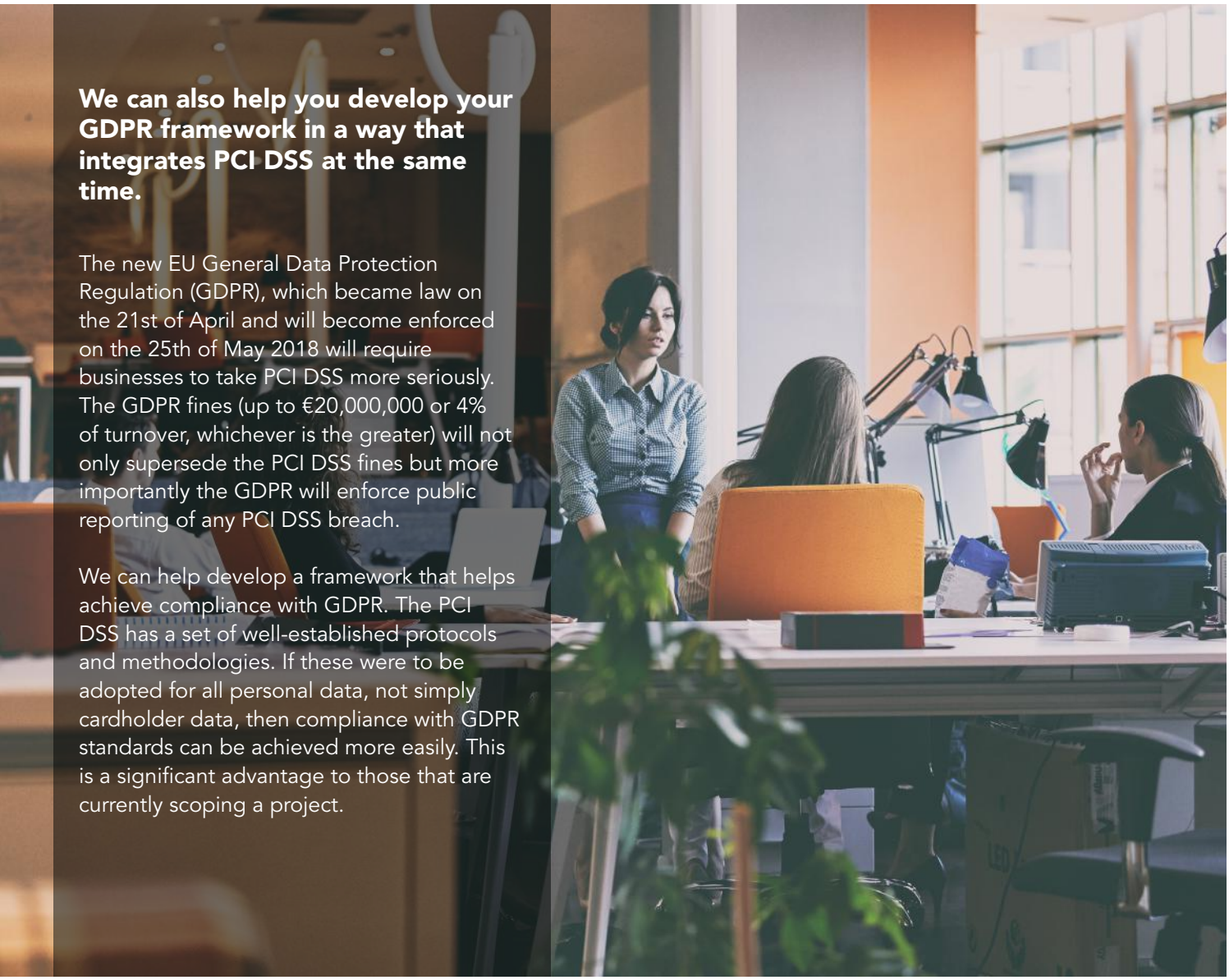
We also offer remediation support for your PCI implementation project, to help your organisation achieve and maintain compliance with the Standard.

IT governance™

Protect • Comply • Thrive

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.

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	

We can help you address all payment requirements

Whether your project is about reducing the cardholder data environment or in-depth testing and reporting, we can help.

IT Governance provides services to support organisations' PCI activities throughout all stages – from building a PCI programme to performing ongoing assessments aimed at improving your security posture. We provide products and services in each of the various compliance categories (criteria below based on those from Visa and Mastercard):

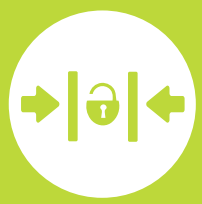
Merchants/service providers	Annual on-site audit	SAQ	Quarterly* external vulnerability scan (ASV)	Quarterly* internal vulnerability scan	Annual** penetration test (Level 2)	Quarterly wireless network analysis	Annual web application vulnerability scan[1]
			Req. 11.2.2	Req. 11.2.1	Req. 11.3	Req. 11.1	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.

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.

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.

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.

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.

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.

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.

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.

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	PCI DSS Implementation Course
Offers an introduction to the PCI DSS and delivers practical guidance on how it applies to your organisation.	A two-day course that covers all aspects of implementing a PCI DSS compliance programme. Successful completion of the included exam leads to the industry-recognised PCI Implementation qualification.

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.

Why IT Governance?

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 QSA audits. We work with our customers to assure PCI compliance while minimising business disruption, keeping costs down and ensuring improved customer engagement.

Our credentials and corporate certificates:

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

t: + 44 (0) 845 070 1750
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

@ITGovernance /it-governance /ITGovernanceLtd