Protect • Comply • Thrive

The PCI DSS:
Challenge or opportunity?

First unveiled in 2004, the Payment Card industry Data Security Standard (PCI DSS) is the result of collaboration between the major credit card brands: American Express, Discover, JCB, MasterCard and Visa. Originally, each of the card companies implemented its own security programme.

By creating the PCI DSS, the companies set out to provide a unified, industry-wide standard.

The PCI DSS was developed to encourage and enhance cardholder data security, and to facilitate the broad adoption of consistent data security measures globally. The card schemes, in reaction to a surge of breaches, sought to ensure that a baseline of security was adopted wherever an entity processed, stored or transmitted cardholder data.

As a general guideline, any merchant or service provider that stores, processes or transmits cardholder data is required to comply with the Standard. The Standard is not law (except in a couple of US states) and non-compliance is not punishable by imprisonment; instead, it's enforced through terms of business as part of the contract between the merchant, acquirer and other payment brands. Organisations that fail to comply are likely to get less beneficial commercial terms (and may even be refused service), and those that suffer a breach and are found to have fallen out of compliance are likely to face significant fines.

As payment card data is considered to be personal data under the current UK Data Protection Act, the ICO has the power to fine organisations for serious breaches of the laws which govern the protection of personal data.

The PCI challenge

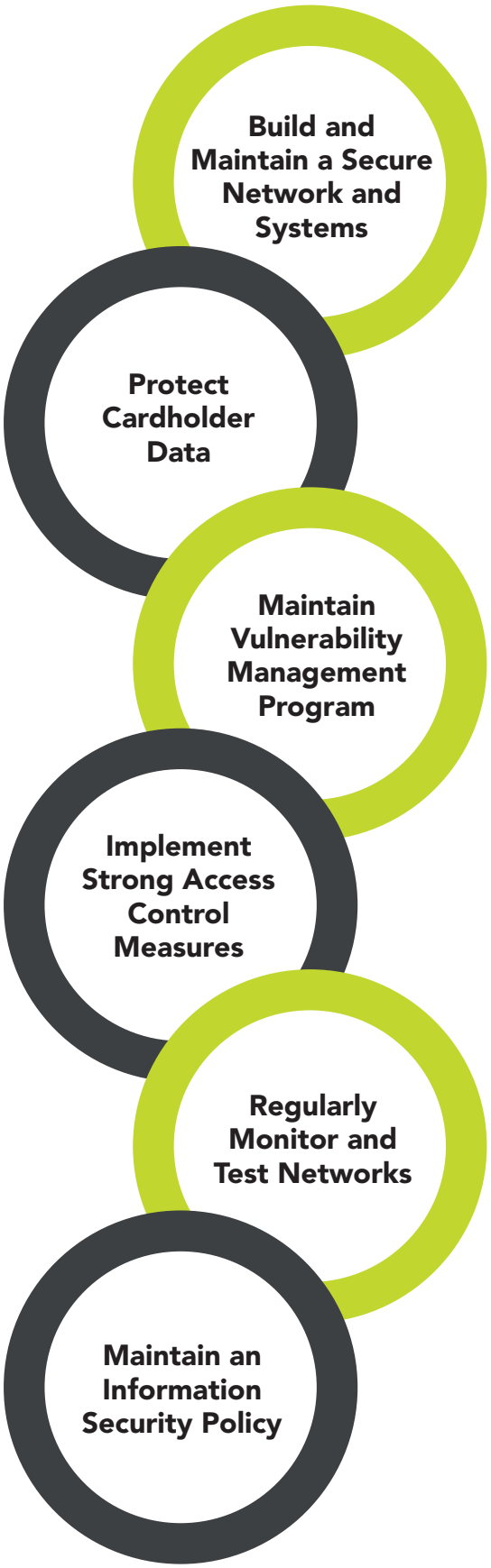
Despite the prospect of fines and penalties, many merchants are not PCI-compliant. There are numerous reasons for this, ranging from a lack of awareness/interest (especially SMEs) to inadequate scoping of the cardholder data environment and underestimating the technical complexity of the Standard, not to mention the general strain caused by having to comply with a broad range of other standards, laws and regulations.

Faced with these challenges, what is the best way to achieve compliance and to ensure that it can be maintained within an acceptable budget? IT Governance believes the most effective approach is not to view the PCI DSS as a compliance burden, but to use it as originally intended – as an information security baseline that provides the organisation with an opportunity to reduce risk.

Focusing on snapshot efforts is neither sustainable nor cost effective, and will work against your organisation's performance in the long run. IT Governance's approach uses the PCI DSS as a set of information security controls that can be effectively integrated within a broader governance, risk management and compliance (GRC) framework to achieve greater efficiencies and further reduce risk.

PCI DSS compliance requirements

The PCI DSS specifies 12 requirements relating to the storage, transmission and processing of cardholder data. These are organised into six control objectives:



1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

5. Protect all systems against malware and regularly update anti-virus software, or programs
6. Develop and maintain secure systems and applications

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

12. Maintain a policy that addresses information security for all personnel

Understanding a business's PCI level

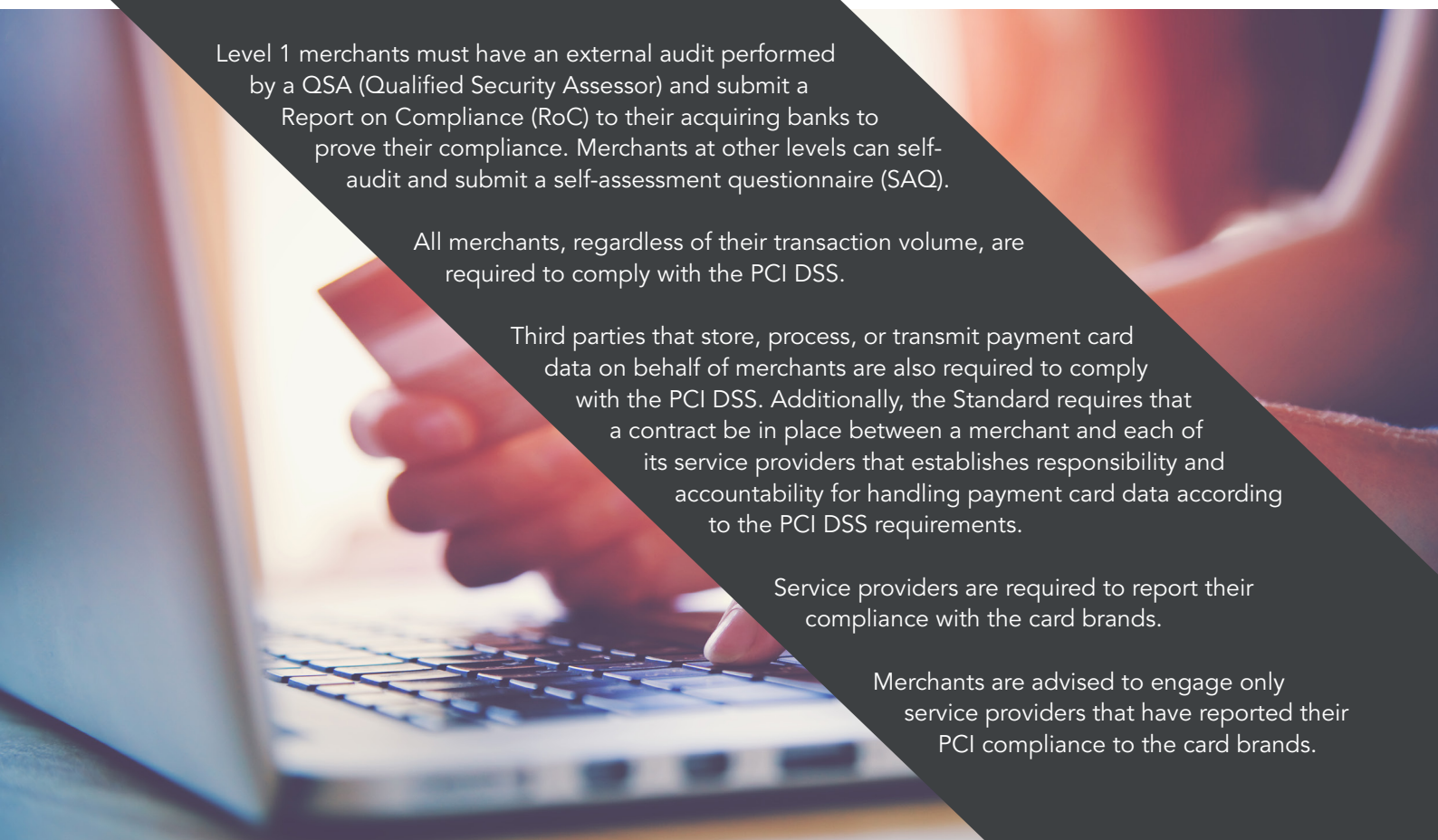
PCI compliance requirements vary depending on the number of card transactions a business accepts.
The following merchant levels apply (criteria are from Visa and MasterCard):

PCI Level 1 — 6 million + transactions per year

PCI Level 2 — 1 million - 6 million transactions per year

PCI Level 3 — 20,000 - 1 million e-commerce transactions

PCI Level 4 — Fewer than 20,000 e-commerce transactions per year (VISA). All other merchants (MasterCard)



Level 1 merchants must have an external audit performed by a QSA (Qualified Security Assessor) and submit a Report on Compliance (RoC) to their acquiring banks to prove their compliance. Merchants at other levels can self-audit and submit a self-assessment questionnaire (SAQ).

All merchants, regardless of their transaction volume, are required to comply with the PCI DSS.

Third parties that store, process, or transmit payment card data on behalf of merchants are also required to comply with the PCI DSS. Additionally, the Standard requires that a contract be in place between a merchant and each of its service providers that establishes responsibility and accountability for handling payment card data according to the PCI DSS requirements.

Service providers are required to report their compliance with the card brands.

Merchants are advised to engage only service providers that have reported their PCI compliance to the card brands.

Why is compliance important?

If implemented correctly, the PCI DSS can help organisations secure their business data. It provides a baseline of security requirements, which lets organisations know what action they should take. One of the benefits of the PCI DSS is that it provides a detailed action plan that can be applied to companies of any size or type and any method of storing payment card data.

The stakes of payment card security should be obvious. According to the Trustwave 2017 Global Security Report, payment card data is targeted in more than half of attacks against commercial environments. Breaches can lead to fines and other enforcement action, as well as significant costs in responding to and rectifying incidents.

Organisations also need to consider the reputational damage of payment card breaches. Customers might choose to stop doing business with you, and you could have a hard time attracting new customers.

Penalties for non-compliance

The consequences of a data breach will be proportionate to the severity of the incident and the extent to which the merchant is able to demonstrate prior compliance with the PCI DSS.

Any merchant that breaches the Standard could face serious consequences, including fines, litigation and reputational damage. They could also:

- Face a significant cost for a forensic investigation;
- Automatically become a Level 1 merchant, which requires yearly on-site audits;
- Be subject to a charge from the issuers and acquirers for reissuing cards; and
- Lose their ability to accept card payments.

The status of compliance

According to Verizon's 2017 Payment Security Report, 55.4% of organisations achieve full compliance with the PCI DSS, but almost half of them fall out of compliance within a year.

Even more telling is that, in every payment card data breach between 2010 and 2016 that Verizon investigated, the affected organisation showed lower levels of compliance with 10 of the 12 key requirements of the PCI DSS.

The fact that organisations weren't consistently maintaining security controls was a key driver for the changes introduced in the PCI DSS v3.2. These focused on helping organisations make sure that critical data security controls remain in place throughout the year and that they are tested as part of an ongoing security monitoring process.

Six major challenges faced by merchants

Scoping the cardholder data environment

Many merchants lack a clear definition of the scope of the payment environment for PCI certification. A scope that's too narrow can lead to cardholder data being compromised, and a scope that's too broad can unnecessarily increase the cost of implementation or even undermine the effectiveness of the whole programme. Trying to do too much will overcomplicate proceedings, leaving your organisation with a false sense of security and liable to neglect the fundamentals – which can be tricky enough in themselves.

Judging the extent and complexity of PCI compliance

The range of activities involved in achieving and maintaining the Standard is broad: there are 243 numbered requirements and 330 testing requirements that all merchants must meet. Most merchants that we support are categorised as Visa or Mastercard Level 3 or Level 4 for reporting purposes. These organisations typically report their compliance using an SAQ. Although the aim of SAQs is to make the process of reporting compliance simpler, we often find that merchants struggle over the correct form to use, and frequently underestimate which portions of their environment are required to be compliant and how to secure those systems.

Regularly testing security systems and processes

Many organisations fall out of compliance because they fail to recognise the importance of regular penetration testing. Requirement 11 of the PCI DSS describes the need to regularly and frequently carry out tests to identify unaddressed security issues and scan for rogue wireless networks. Regular testing is fundamental to making sure that an organisation is prepared for new and evolving attacks, but according to Verizon's 2017 Payment Security Report, organisations struggle more with this requirement than any other. Many organisations perform little or no regular testing on the adequacy of the security controls governing their network and Internet-facing applications, which can leave back doors for criminal hackers to exploit.

Documenting PCI policies and procedures

Security policies should be implemented to address an organisation's weakest link: its staff. If employees don't know or understand what's expected of them, they run the risk of exposing cardholder data.

Logging and auditing systems

Requirement 10.6.1 of the Standard, which mandates a daily review of security events and logs, creates several challenges. Failing to maintain logging solutions can bring down an organisation's compliance percentage – whether that's down to technical, budgetary or human resource restrictions. It also puts additional pressure on those responsible for managing systems that need to be logged. Breaches are more likely to go undetected longer when an environment isn't actively monitored. Organisations should create and practise the necessary procedures to protect data and warn of abnormal behaviour in an environment that interacts with sensitive data.

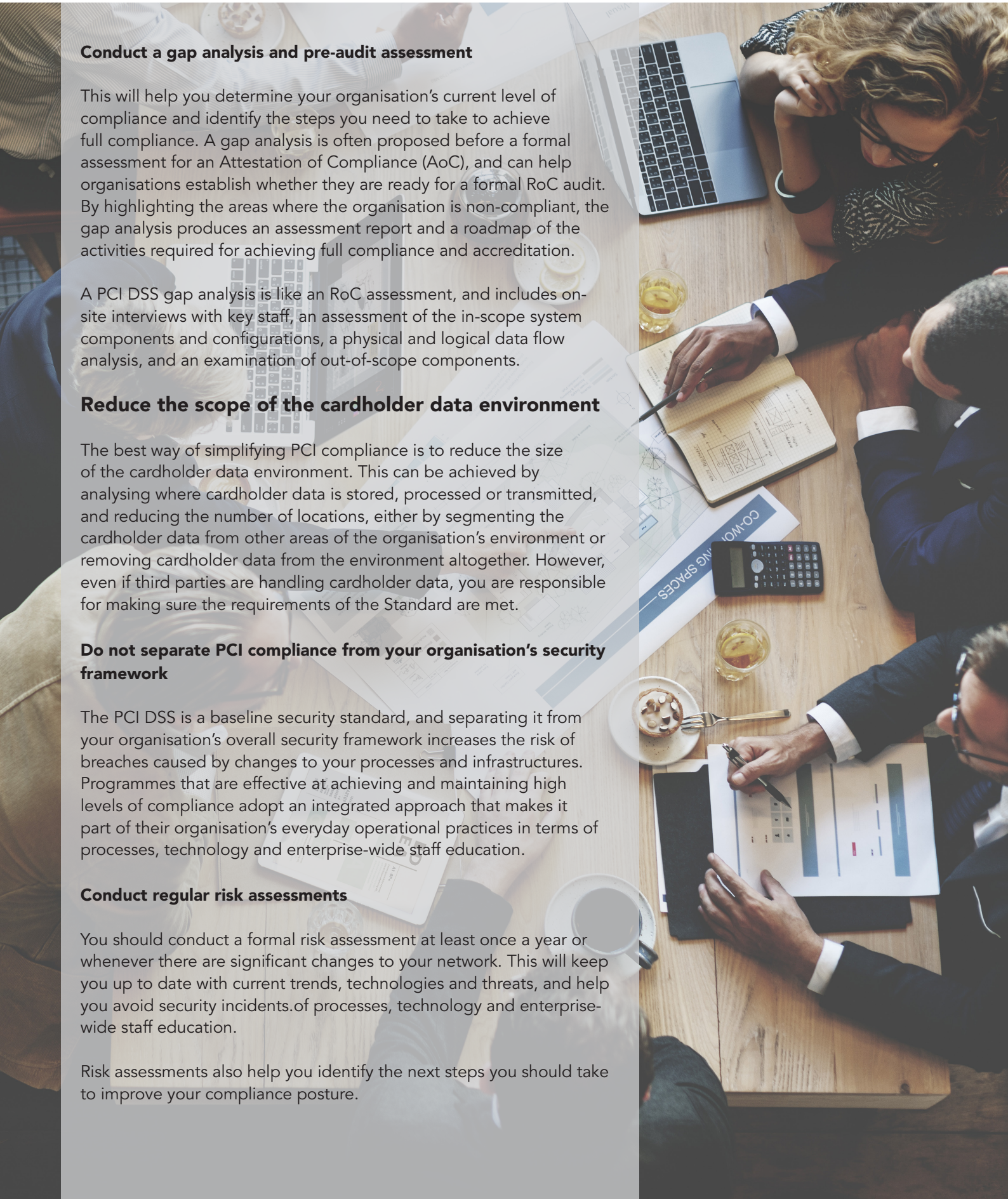
Protecting stored payment card data

Requirement 3 details technical guidelines for protecting stored cardholder data and the requirements for encryption. At a minimum, the Standard requires the primary account number to be rendered unreadable anywhere it is stored, including portable digital media, backup media and logs. But even with the significant security that encryption provides, it is not without its technical challenges. Operating system and application vendors haven't made it easy and seamless to implement encryption, especially because of a lack of support for legacy systems.

Recommendations on managing the PCI DSS more effectively

Achieving and maintaining compliance with the PCI DSS is not straightforward: if you make mistakes when implementing the Standard's requirements, you leave yourself vulnerable to data breaches and regulatory fines.

Here are some recommendations to help achieve and maintain PCI DSS compliance more effectively.



Conduct a gap analysis and pre-audit assessment

This will help you determine your organisation's current level of compliance and identify the steps you need to take to achieve full compliance. A gap analysis is often proposed before a formal assessment for an Attestation of Compliance (AoC), and can help organisations establish whether they are ready for a formal RoC audit. By highlighting the areas where the organisation is non-compliant, the gap analysis produces an assessment report and a roadmap of the activities required for achieving full compliance and accreditation.

A PCI DSS gap analysis is like an RoC assessment, and includes on-site interviews with key staff, an assessment of the in-scope system components and configurations, a physical and logical data flow analysis, and an examination of out-of-scope components.

Reduce the scope of the cardholder data environment

The best way of simplifying PCI compliance is to reduce the size of the cardholder data environment. This can be achieved by analysing where cardholder data is stored, processed or transmitted, and reducing the number of locations, either by segmenting the cardholder data from other areas of the organisation's environment or removing cardholder data from the environment altogether. However, even if third parties are handling cardholder data, you are responsible for making sure the requirements of the Standard are met.

Do not separate PCI compliance from your organisation's security framework

The PCI DSS is a baseline security standard, and separating it from your organisation's overall security framework increases the risk of breaches caused by changes to your processes and infrastructures. Programmes that are effective at achieving and maintaining high levels of compliance adopt an integrated approach that makes it part of their organisation's everyday operational practices in terms of processes, technology and enterprise-wide staff education.

Conduct regular risk assessments

You should conduct a formal risk assessment at least once a year or whenever there are significant changes to your network. This will keep you up to date with current trends, technologies and threats, and help you avoid security incidents.of processes, technology and enterprise-wide staff education.

Risk assessments also help you identify the next steps you should take to improve your compliance posture.

How compliance with the PCI DSS can help you to meet the requirements of the GDPR

The EU General Data Protection Regulation (GDPR), which became law on 24 May 2016 and will be enforced from 25 May 2018, will make information security more of a priority for organisations, which will have the effect of making businesses take the PCI DSS more seriously.

Under GDPR, it is a legal requirement that all personal data breaches are reported to the Information Commissioner's Office (ICO) within 72 hours. Failure to report breaches attracts fines up to 10 million euros or 2% of annual turnover. Breaches, which occur through failures to comply with the sixth data protection principle (maintaining confidentiality and integrity of personal data) can attract fines up to €20 million or 4% of annual turnover (whichever is the greater). Inadequate or non-implementation of PCI DSS is likely to be treated, by the ICO, as negligence and any card holder data breach will therefore, in addition to fines and penalties from acquiring banks, attract GDPR monetary penalties.

If your organisation is PCI DSS compliant then you will already be conducting annual reviews of the cardholder data that you process. This aims to ensure that any new technology you've introduced or new processes you've implemented are included within your PCI DSS compliance. This schedule of reviews gives you a framework that can also be used when implementing a GDPR compliance project, giving you an advantage over those organisations that are yet to comply with the PCI DSS.

Likewise, if you're PCI DSS compliant then your organisation will have invested in secure technologies, antivirus software, encryption, strong access control measures, testing, logging and monitoring. When you have identified the additional personal data your organisation needs to protect under the GDPR, then you could already have many of the technologies, processes and procedures necessary to protect it.

First steps to compliance

You will probably have two major concerns when implementing the PCI DSS: how much will it cost and how long will it take? You will obviously want to reduce the cost and time as much as possible, but you don't want to cut corners along the way.

1. The key to a successful compliance project is to be able to identify the steps you need to take to fill any compliance gaps. You should start by documenting your cardholder data environment. Mapping the data flow of the environment will help you identify its scope. This will involve documenting the steps of the transaction process and all the network components the data encounters.

2. The next step is to create a PCI DSS team, comprising both technical and non-technical personnel. The technical members should start by running approved scanning vendor (ASV) scans on IPs and benchmarking security settings and security products against the Standard.

3. Meanwhile, the compliance team should prepare a gap analysis to review and analyse the organisation's policies, procedures, configurations and data flow diagrams.

4. Putting together the results of the scans and the technical benchmarking will allow the team to create a remediation map showing which tasks can be assigned to the relevant people.

5. Contracting a QSA can also help. Merchants aren't required to hire a PCI-certified QSA, but doing so could cut costs and resources, which would help the organisation achieve compliance faster. A QSA also helps organisations make the most of what they already have in their security environment and gives them the assurance of a third-party assessment.

About IT Governance's PCI DSS practice

We will help you achieve and maintain PCI compliance by tackling the challenges of scoping the cardholder data environment, reducing the complexity of card data flow, testing and protecting stored payment card data.

Whether you are a merchant or service provider, a large entity or a small enterprise looking to achieve and maintain compliance with the PCI DSS, IT Governance can help. As an authorised QSA company, we will assess your needs, carefully explain the PCI compliance requirements relevant to you, and provide solutions that will suit your budget.

Assess your current PCI compliance posture and produces a strategic roadmap that can be implemented to achieve full compliance with the Standard.

A PCI DSS gap analysis will help your organisation prepare to pass the annual audit. A PCI gap analysis helps you use PCI compliance as the starting point for defining and implementing a security strategy.

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.

Identify the right SAQ to complete and achieve full compliance with the PCI DSS.

PCI SAQs can make compliance easier for organisations with lower transaction volumes, but it's helpful to have the guidance of PCI industry experts to ensure your responses are in line with each requirement.

A fully documented ROC that is accepted by your business partners.

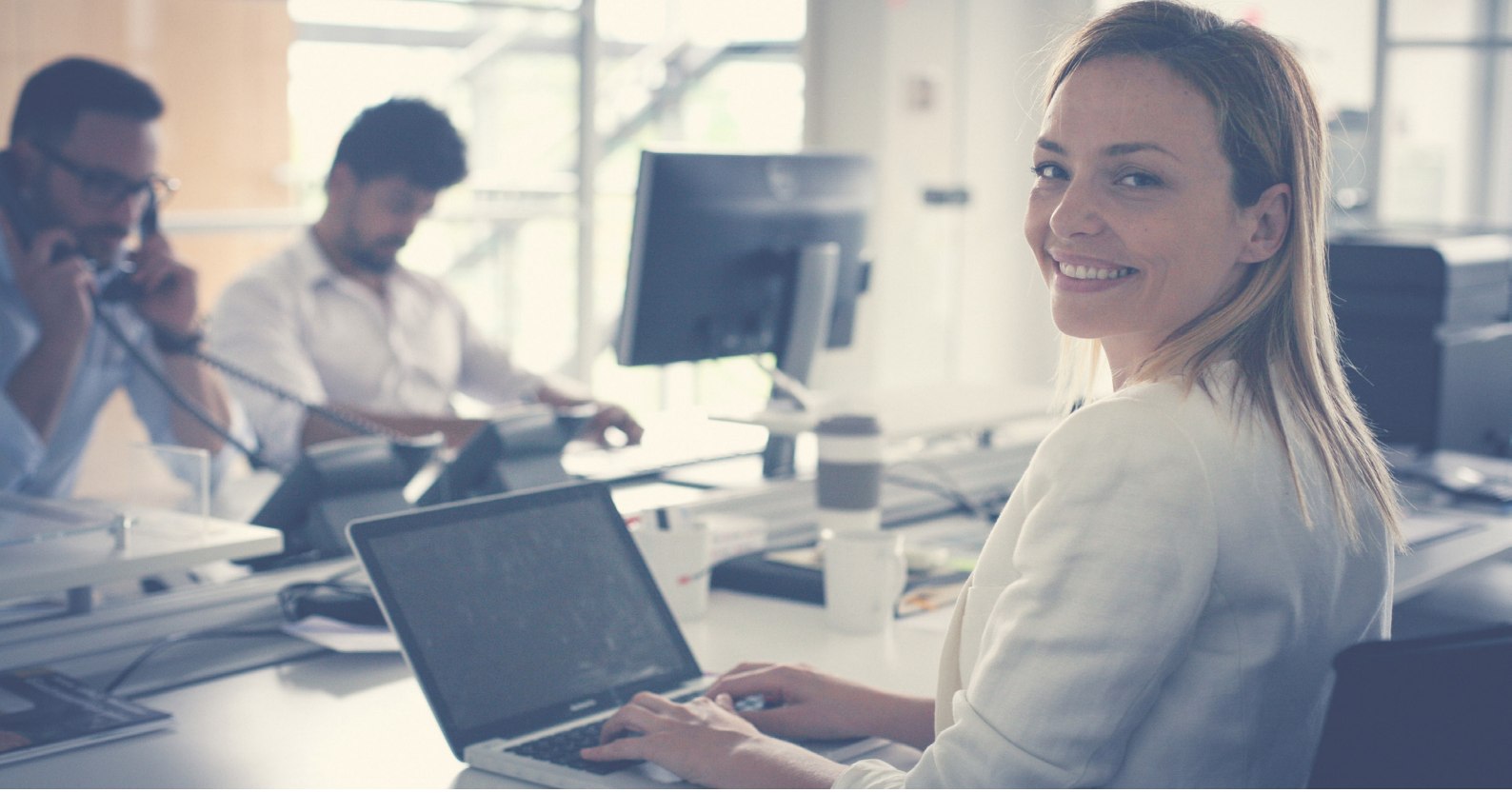
A PCI Report on Compliance (ROC) is required by organisations with large transaction volumes, and must be conducted by a Qualified Security Assessor (QSA) who will issue a formal report to the PCI Security Standards Council to attest that your organisation is in full compliance.

Retain compliance once it has been achieved.

PCI DSS remediation can be both time consuming and resource intensive. A well-structured and proven PCI remediation plan significantly helps organisations reduce the time and cost needed to achieve compliance.

Streamline your documentation requirements.

Designed by a leading PCI QSA, our documentation toolkit contains all the expert guidance, advice and fully customisable documentation templates you will need to accelerate your PCI DSS project.



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:

Our PCI 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)333 800 7000
e: servicecentre@itgovernance.co.uk
w: www.itgovernance.co.uk

/ITGovernanceLtd /ITGovernanceLtd /ITGovernanceLtd