



Payment card industry  
data security standard  
Reassuring systems

---

# Does your company store, process or transmit cardholder data?

## Introducing PCI DSS

Following a series of high profile data security breaches consumers who use payment cards are increasingly concerned about the security of their personal and financial data and the risk of fraud. Driven by a need to reassure cardholders the payment card schemes have developed the Payment Card Industry Data Security Standards (PCI DSS) as a minimum standard for all organisations that process store or transmit card details.

Deloitte offers a comprehensive set of services to deliver the required security and fraud management processes needed for compliance with the necessary real world experience that can limit the overall impact of implementing the requirements of the standard.

## Who does this affect?

Whilst initial focus of the standard was primarily online transactions the PCI DSS now applies to any organisation that stores, processes or transmits cardholder data. This includes bricks and mortar mail and telephone order, and eCommerce retailers, as well as the third party service providers that support them, such as payment processors and hosting providers.

## Why comply?

The card schemes insist on PCI DSS compliance to demonstrate that cardholders' data is secured. Organisations who are not PCI DSS compliant face potential fines and could ultimately risk losing their ability to process card payments.

However, by complying with the PCI DSS, a merchant or payment processor can benefit in a number of ways, including:

- Demonstrating to customers that management takes customer information security seriously and

have effective controls in place over account and transaction information.

- Providing a competitive edge in helping to maintain a positive brand image and enhancing trust to attract future customers.
- Providing the respective Regulator(s) with assurance that processes are suitably controlled.
- Offering exemption from penalties, fees or fines that may be issued by the card schemes after a security incident, providing proper controls were in place and appropriate actions followed.
- Increasing awareness of security within the organisation.
- Increasing IT efficiency and potential cost savings (e.g. through improved patch management anti-virus controls, user account management, etc).

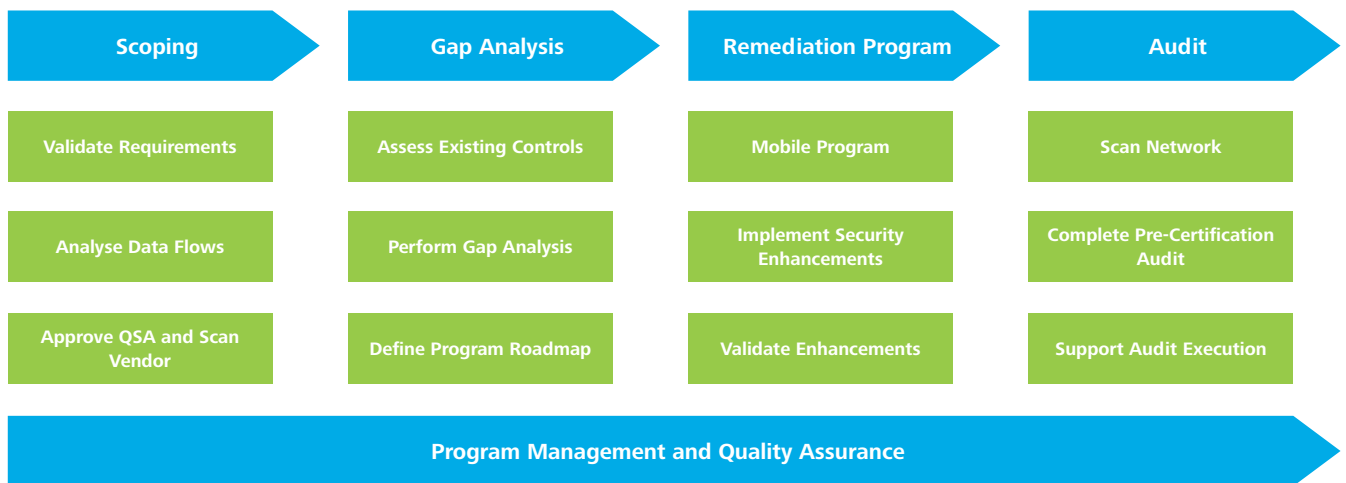
## How to achieve compliance

The PCI DSS is a multifaceted security standard comprising twelve high-level requirements split into the following categories:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

PCI DSS places extensive demands across a variety of areas and any remediation program will touch on people, process, technology and governance controls. This is an organisation wide issue and hence any response needs to be coordinated as such.

We are experienced in helping organisations achieve compliance with the PCI DSS and have developed a 4-stage program as shown in the diagram overleaf.



### 1. Scoping

We identify the steps you need to take to become PCI DSS compliant, assess the number of system components that handle cardholder data and look at minimising the number of people and processes that have access to the data. This presents security and operational advantages from the outset and may result in a scope reduction for the compliance program.

### 2. Gap analysis

We benchmark your current technical policy and procedural controls against the standard, and then form a prioritised, tailored action plan based on factors such as their relative urgency for risk mitigation quick wins and their complexity.

### 3. Remediation program

We help you divide your remediation program into manageable projects, before helping you mobilise resources to address the work. We have experience in the implementation of projects likely to make up your compliance program and can assist with program leadership, resource shortfalls or advisory support.

### 4. Audit

We can also support the certification process by conducting a pre-certification audit and helping to coordinate the vulnerability scans that are required for compliance.

### Why Deloitte?

Our Security and Privacy Practice has, through engagements with a range of clients in a variety of sectors built up a wealth of knowledge on the standard how it needs to be applied and how to maximise benefit whilst minimising impact. We feel the following have been important contributors in our success in assisting our clients with their PCI DSS programs:

- Breadth and depth of skills - We have a large pool of resources with a broad and deep set of skills allowing us to address all of the issues presented by a PCI DSS compliance program.
- Practical implementation experience - We are experienced in delivering complex security remediation programs which involve people process and technology change.
- Rigorous program management skills - We are able to leverage the substantial program management experience and expertise that we have within Deloitte.
- Collaborative approach to delivery - We believe that working closely with our clients and their partners is very important to the success of any PCI DSS program.

## Here to meet your needs

### Malta contacts:

#### Ashraf Fahmy

Leader Enterprise Risk Services  
Tel + 356 23432000  
asfahmy@deloitte.com.mt

#### Stephen Paris

Leader Financial Services  
Tel + 356 23432000  
sparis@deloitte.com.mt

Deloitte Place, Mriehel Bypass, Mriehel BKR3000, Malta  
Telephone: (+356) 2343 2000  
Facsimile: (+356) 2134 4443  
www.deloitte.com/mt

#### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte Malta refers to a civil partnership constituted between limited liability companies, and its affiliated operating entities; Deloitte Services Limited and Deloitte Audit Limited. The latter is authorised to provide audit services in Malta in terms of the Accountancy Profession Act.

A list of the corporate partners, as well as the principals authorised to sign reports on behalf of the firm, is available at [www.deloitte.com/mt/about](http://www.deloitte.com/mt/about).

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.