

# PCI DSS BASICS

## WHAT IS PCI DSS AND WHY DO YOU NEED TO COMPLY?

### WHAT IS THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)?

Each of the payment brands has a set of information security requirements that must be met by its merchants. This means that in order to process VISA transactions you needed to comply with Visa's Cardholder Information Security Program (CISP). When dealing with MasterCard you needed to comply with MasterCard's Site Data Protection (SDP).

In order to simplify the requirements on merchants and to align the different programs the founding members developed PCI DSS, and the PCI Security Standards Council, who manages the various different standards, was created.

### WHAT ARE THE DIFFERENT STANDARDS?

There are three standards under the management of the PCI SSC: The Payment Card Industry Data Security Standard (PCI DSS), the Payment Application Data Security Standard (PA DSS) and the Payment Card Industry PIN Transaction Security (PCI PTS).

- PCI PTS applies to manufacturers or vendors of devices such where a user enters a PIN. For example the EFTPOS machines used in supermarkets and petrol stations.
- PA DSS applies to applications that are provided for sale that accept, process, store or transmit credit card details. For example if you have created and are selling an application to take credit card payments, then the application will likely need to comply with PA DSS.
- PCI DSS is the overall standard and is the framework for information security that needs to be in place in an organisation. There are 12 requirements that each address a specific aspect of information security risk.

As merchants and service providers you will likely need to comply with PCI DSS.

### WHO NEEDS TO COMPLY WITH PCI DSS?

PCI DSS applies to all organisations that accept, process, store or transmit credit card information.

It does not matter how small or large you are, you have to meet all the requirements of PCI DSS, although there are some small differences in the standard depending on whether you are a merchant or a service provider. The difference lies in the validation requirements, i.e. how your compliance is verified.

Each payment brand has a set of criteria that determines the level of merchant you are. Typically the number of credit card transactions you process dictates your validation requirements. These include quarterly vulnerability scans, completion of self-assessment questionnaires or on-site assessments by a Qualified Security Assessor (QSA).

### WHAT DO YOU HAVE TO DO?

The validation requirements depend on your level, but one requirement is common to all levels, which is the external vulnerability scans. An Authorised Security Vendor (ASV) must perform these scans on any Internet facing infrastructure.

If you process more than 6 million MasterCard or Visa transactions or more than 2 million American Express transactions<sup>1</sup>, then you will be considered a level 1 merchant or service provider and in addition to the scan, you will also be required to have an on-site assessment performed by a Qualified Security Assessor (QSA).

As a Level 2 merchant or Service Provider you will likely be processing between 1 million and 6 million transactions per year for MasterCard or Visa. You will be required to complete a self-assessment questionnaire or you can elect to conduct an on-site assessment.

A Level 3 Merchant or service provider is typically just required to complete a self-assessment questionnaire.

While the levels are a good guide, the acquiring bank may classify an organisation into a different level.

---

<sup>1</sup> Be aware that these criteria change occasionally.

## WHY SHOULD YOU COMPLY?

PCI DSS introduces a base security level. By complying with the standard you are implementing information security best practices and you will improve the overall security of the organisation.

Customers have more confidence that you are treating their credit card information appropriately.

However, more importantly, you reduce costs - not just by avoiding increased fees and potentially fines or even lawsuits, but also by having a more manageable and robust environment.

## PCI COMPLIANCE CHECKLIST

The following checklist will help you to understand the requirement for PCI compliance within your organisation:



Can your customers pay for any goods or services using a credit card? (online, or in stores)	
Do you use credit card details for any of your business processes? (customer identity verification, batch payment processes, etc)	
Do you store credit card details anywhere in your organisation, electronically or on paper?	
Do you receive or transmit credit card details from anyone or to anyone?	
Has your acquiring bank or the payment brand told you that you have to comply with PCI DSS?	

If the answer to any of the above is "yes", then you will need to comply with **all** the requirements of PCI DSS and validate according to your particular level.

Once you have identified that you need to comply, you need to map out how credit card information is processed:



All the channels through which you accept credit cards? <ul style="list-style-type: none"> <li>Do you accept cards via your ecommerce site, paper forms, faxes, emails, file transfers?</li> </ul>	
What happens next with the credit card details? <ul style="list-style-type: none"> <li>Are they sent to a payment gateway?</li> <li>Are they stored in a file and sent off?</li> <li>Do you scan in forms?</li> <li>How are transactions authorised?</li> <li>How are charge backs and settlements handled?</li> </ul>	
How do you process credit cards and how is the information used?	
Who has access to the credit card details? <ul style="list-style-type: none"> <li>Customer Sales Representatives, Finance people, IT personnel, others?</li> </ul>	
How are credit card details stored? <ul style="list-style-type: none"> <li>Are they encrypted?</li> <li>Are they truncated (i.e. only store the first 6 and last 4 numbers)</li> <li>Are they tokenised (format change so not resembling a credit card number and irreversible)</li> <li>Do you back the information up?</li> <li>Are credit card details stored on USB or Thumb drives?</li> </ul>	

Once you have identified the answers you will have a clear picture of the credit card flows within your organisation. You are now in a good position to look at how those systems are managed, find the gaps and take steps to fix any issues.

## WHAT HAPPENS IF YOU DO NOT COMPLY?

That will depend on the acquiring bank. The bank may impose additional fees on your organisation until you are compliant, or they may refuse services.

In the event of a breach you may be held liable for all costs, this includes the costs of the investigation, but also issuing of replacement cards and all other associated costs with the breach.

## ABOUT SHEARWATER

Shearwater Solutions (Shearwater) is an Information Security Specialist with proven experience in the field. Shearwater's philosophy is to partner with its clients to achieve operational and strategic success within the information security operations. Partnership at Shearwater are characterised by mutual benefit and tend to be long term in nature. Shearwater has a diverse client base across multiple industries including Government (Federal, State and local) and Enterprise (Finance, Retail, Manufacturing, Telecommunications and Service Providers).

Level 1, 6 Spring Street  
Chatswood  
NSW 2067  
Australia  
**Phone:** +61 2 9488 4600  
[www.shearwater.com.au](http://www.shearwater.com.au)

## ABOUT MACQUARIE TELECOM

Founded in 1992, Macquarie Telecom (ASX:MAQ) is Australia's number one Managed Hosting and business-only telecommunications company.

Working with and supporting some of Australia's best-known organisations, Macquarie Telecom is a full service hosting provider offering managed dedicated servers, managed co-location, and managed private and public clouds for mid-size businesses, corporate and government IT departments.

Level 20, 2 Market Street  
Sydney NSW 2000  
**Phone:** +61 2 8221 7777  
**Freecall:** 1800 004 943  
[www.macquarietelecom.com](http://www.macquarietelecom.com)