

Whitepaper

Simplifying the Payment Card Industry Data Security Standard

A Security-Assessment.com Publication

Special points of interest:

- Visa research found that "...theft or loss of personal financial information is the number one concern among consumers".

11 September 2006

- The PCI Security Standards Council says companies should look at PCI DSS as a way to avoid large breaches instead as a list of rules to heed to keep the compliance policy at bay.

April 2007

searchsecurity.com

In this Paper

Abstract	1
How does the PCI DSS impact Me	2
Where does my organisation fit in	2
PCI DSS Requirements	3
Audit Requirements	3
The Self Assessment Questionnaire.	4
Onsite Audits	4
PCI Service Offerings	5

Abstract

The Credit Card Payment System, while convenient, is a fraught with financial, reputational and regulatory risks associated with Credit Card theft and fraud. It is a serious problem for Merchants and Consumers and one that the Payment Card Industry takes very seriously.

In response to the growth of credit card fraud, identity theft and other credit card associated crimes, the Payment Card Industry have developed *The Payment Card Industry Data Security Standard* (PCI DSS).

Poorly secured systems result in opportunities for cardholder and transaction information being exposed.

The PCI DSS was established to provide a level of control and assurance around how organisations processing, storing and transmitting credit card holder and transaction information must protect this information from the risks of credit card associated crime.

Organisations that do not comply with the PCI DSS face sanctions that include monetary fines, heavier audit requirements and exclusion from the Payment Card Industry.

The Payment Card Industry Data Security Standard (PCI DSS) contains minimal level mandatory practices required to protect cardholder information.

The PCI DSS was developed by the Payment Card Industry and defines 12 principle security requirements.

These principles must be implemented by credit card merchants and service providers to satisfy the terms of payment card associations

Although an organisation's acquiring bank is required to notify organisations of their requirements for PCI Compliance and how it will affect them, few organisations fully understand what these



requirements actually are.

Frustrated with the slow rate of compliance, Mastercard have already begun imposing monetary fines.

Becoming PCI compliant will require significant effort for many as the PCI DSS is not just another 'tick the box' standard with minimalist guidelines. But it should not be considered just an exercise in keeping the policy police at bay.

In our opinion, implementing the PCI DSS standards should in fact be considered as conventional 'good security practice' that help organisations avoid large breaches.



How does the PCI DSS Impact Me



Organisations that accept, process or store credit card information **must** be compliant with the PCI DSS².

Organisations must ensure that their network, environment, applications and associated business processes are implemented and maintained to rigid standards to protect credit card and cardholder information.

For most organisations becoming and maintaining compliance to the PCI DSS will involve a process of assessing the environment against the standard and then identifying and fixing security gaps.

The PCI DSS can have a large impact upon organisations who do not have a well defined and

implemented IT Security Strategy and supporting policies and standards. Organisations should not underestimate the impact of the PCI DSS.

Organisations need to put in place a program of continuous assurance to ensure that the standard is maintained and complied with on an ongoing basis.

With new emphasis on enforcing these standards both merchants and service providers need to be aware of, understand and comply with these standards.

By meeting the terms of PCI compliance, companies will reduce their regulatory, reputational and financial risks associated with security breaches and cardholder information being

compromised.

Companies who fail to be compliant with these standards may face penalties such as heavy fines and restrictions as well as possible exclusion from credit card acceptance programs.

In Australia, organisations will find PCI DSS a challenge. While the standard contains good practices that organisations should be adopting anyway the impacts will be significant as Australian businesses have never felt regulatory controls this tight before.

PCI Terminology

QSA³—A Qualified Security Assessor (QSA) is a specialist security auditor that has undergone rigid assessment by Visa to perform onsite audits and PCI assessments.

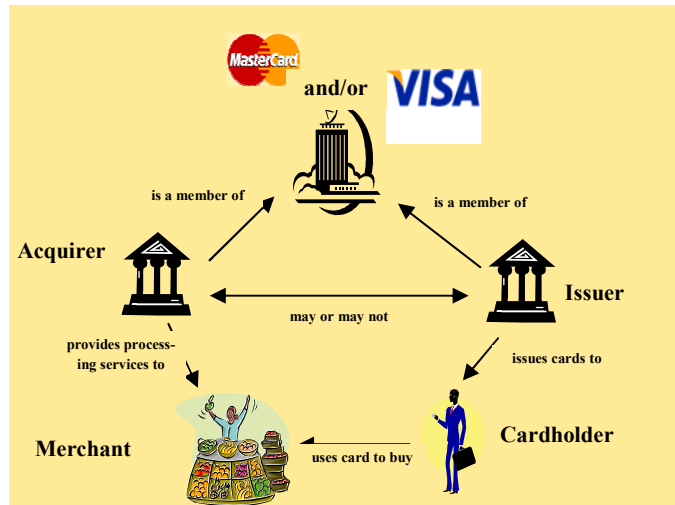
ASV⁴—Approved Scanning Vendor (ASV) is a provider certified by MasterCard to carry out quarterly network security scans

Where does my organisation fit in

The responsibilities and requirements for PCI compliance vary according to the position an organisation holds in the payment card process.

Participants are categorised according to their role in this process and it is important to understand who is who in order to know what the requirements are.

Members of payment card brands such as Visa and MasterCard are classified as either Acquirers or Issuers and in some cases both. Acquirers deal with merchants who are the entities that accept card transactions, whilst the Issuers issue cards to cardholders. Service providers provide services that facilitate acceptance, processing, transporting and storing of card information on behalf of a payment card brand, their members or cardholders.



Now that it is clear who is who, it is essential to understand the requirements in relation to PCI compliance. Acquirers are required by Visa and MasterCard to ensure that their Merchants and Service Providers are compliant with PCI DSS. In cases where non-compliance is revealed Visa and MasterCard can pass

on heavy fines to their Acquirers which can consequently be passed on to the Merchant or Service Provider as well as having restrictions placed on them by the Acquirer. Thus, it is crucial for Merchants and Service Providers to fully understand what their requirements are for PCI DSS compliance

"..only 49 per cent of Australian merchants are aware of the international standard on payment security "

VISA, 11 September 2006



1 Payment Card Industry
 2 Data Security Standard
 3 Qualified Security Assessor
 4 Approved Scanning Vendor

PCI Data Security Standard Requirements

The PCI DSS consists of 12 security requirements that must be adhered to by merchants and service providers that store, process and transmit credit card holder and transaction information.

These requirements are categorised into six sections that address various areas of security controls including technical, administrative and physical security measures. Unlike many standards the PCI DSS defines very detailed implementation baselines.

When assessing PCI it is important to review the requirements within the context of the complete control specifications, not just the high level summary to ensure that the requirements are entirely understood and the correct steps are taken towards compliance.

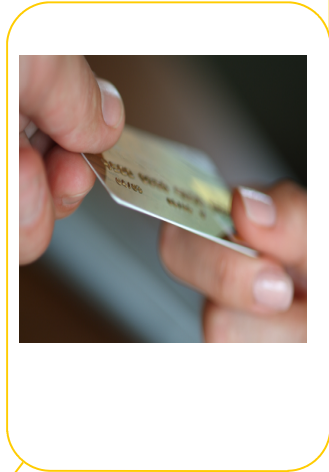
The PCI DSS consists of technical, administrative and physical requirements.

Technical requirements define components such as firewall configurations,

password rules and encryption processes to name a few.

Administrative requirements define the need for an Information Security Policy and administrative controls to support the policy.

Physical security measures are also outlined in the standard to protect cardholder information. These measures include physical locks, security cameras and authorisation procedures for personnel to name a few.



Compliance Requirements

All organisations that process credit card information must be compliant with the PCI DSS. The level of compliance reporting though differs depending on the number of and dollar value of credit card transactions as defined below. In addition, at the discretion of PCI members, a merchant or service provider could be classified at a level different to their transaction level.

Merchant Requirements	Description	Self Assessment Questionnaire	Network Security Scans	QSA Onsite Review
	Level 1	Merchant processing over 6,000,000 transactions or compromised in the last year*	Not Required	✓ (quarterly)
Level 2	Merchant processing between 150,000 and 6,000,000 e-commerce transactions per year*	✓ (annually)	✓ (quarterly)	Not Required
Level 3	Merchant processing between 20,000 and 150,000 e-commerce transactions per year*	✓ (annually)	✓ (quarterly)	Not Required
Level 4	Merchant processing less than 20,000 ecommerce transactions per year and all other Merchants processing up to 6,000,000 transactions per year	RECOMMENED (annually)	RECOMMENED (annually)	Not Required

* Or identified by another payment card brand as this

Service Provider Requirements	Description	Self Assessment Questionnaire	Network Security Scans	QSA Onsite Review
	Level 1	Any Service Provider that processes, stores or transmits over 600,000 transactions or accounts annually for Visa, or processes card data at all or stores card data for Level 1 or 2 Merchants for MasterCard	Not Required	✓ (quarterly)
Level 2	Any Service Provider that - is not in Level 1 and stores, processes or transmits more than 120,000 accounts or transactions annually for Visa, or stores card data for Level 3 Merchants	✓ (annually) For Visa	✓ (quarterly)	✓ (annually) For MasterCard
Level 3	Any Service Provider that stores, processes or transmits less than 120,000 accounts or transactions annually for Visa, or All other Data Storage Entities not in Levels 1 or 2 for MasterCard	✓ (annually)	✓ (quarterly)	Not Required

49 percent of Australian merchants are aware of the international standard on payment security, known as the Payment Card Industry Data Security Standard (PCI DSS). This standard has been promoted by the payment card schemes for some years.

Visa Research

The PCI Data Security requirements:

- ✓ Build and maintain a secure network
- ✓ Protect cardholder data
- ✓ Ensure the maintenance of vulnerability management programs
- ✓ Implement strong access control measures
- ✓ Regularly monitor and test networks
- ✓ Ensure the maintenance of information security policies.
- ✓ PCI Security Standards Council

The Self Assessment Questionnaire

The PCI DSS Self-Assessment Questionnaire is a 'checklist' to ensure all entities that store, process, or transmit Visa cardholder data meet PCI Data Security Standard.

The questionnaire is divided into six sections. Each section focuses on a specific area of security, based on the requirements included in the PCI Data Security Standard.

Questions are yes/no and responding 'no' to any of the question is an area of non-compliance that must be addressed and resolved.

One common mistake organisations make is not assessing question responses within the context to the complete PCI DSS. For example it is not sufficient for an organisation to just have a firewall in place it must be in accordance with the baselines defined in the PCI DSS

While all merchants and service providers must comply with the PCI DSS, completing the Self-Assessment questionnaire is only mandatory for level 2 and level 3 merchants and service providers.

Level 1 merchants and service providers do not have to complete the questionnaire as they must undergo an onsite audit, nor do level 4 merchants and service providers, although it is recommended.

Regardless of whether it is a mandatory requirement for PCI compliance, the self assessment questionnaire is a useful and effective measure of PCI compliance and can be used as a proactive assessment of security control gaps and weaknesses..

While the self assessment questionnaire does not have to be completed by a QSA or ASV it may prove worthwhile to seek assistance in understanding and defining your organisations PCI DSS compliance scope and review requirements.

Network Vulnerability Scanning

A vulnerability assessment is an assessment of an organisations systems for vulnerabilities and can be done on the external internet facing environment or the internal network.

A vulnerability is a system weakness that can be exploited to obtain unauthorized access to cardholder and transaction data. The purpose of vulnerability assessments is to proactively identify and remediate threats before exploitation can occur.

To be compliant with PCI DSS, quarterly vulnerability assessments must be performed on the external

facing environment by an ASV (Approved Scanning Vendor). The Scope of scanning includes all active internet-facing IP Addresses, filtering devices, and web servers that touch the credit card acceptance, transmission and storage process.

If a level 3,4 or 5 vulnerability is found during a PCI Scan, the company will not receive a passing PCI Scan report.

Following a vulnerability assessment, the ASV will provide the organisation with a compliance report. This report must be in the

defined format and be submitted according to the payment card company's requirements. In general the report will outline any vulnerabilities identified, analysis of any related issues as well as offer advice on how to resolve them.

Vulnerability scanning should be regarded as a fundamental component of an overall Vulnerability Management Program.

Network Scan Reports provides organisation with the status of their security risks posture and provides an opportunity to proactively fix network issues to prevent vulnerabilities being exploited.

77 percent of Australian merchants are most concerned about protecting cardholder data, with card fraud the second highest area of concern (40 percent of merchants) and identity theft the third major worry (33 percent).

Visa Australia

Onsite Audits

An Onsite Audit is a detailed assessment of the card processing environment against the 12 PCI DSS requirements. The audit is required to be completed annually by a QSA and submitted to your acquirer.

The PCI onsite audit examines an organisations security controls to determine whether they meet the requirements of the PCI DSS. Determining the

effectiveness of firewalls, ensuring the use of continually updated anti-virus software and ensuring that secure measures are put in place to restrict physical access to data are just a few of the security measures which will be analysed.

The PCI onsite audit must be carried out and reported in accordance with detailed PCI Audit Procedures. The

QSA will assess whether the particular requirements have been implemented appropriately and will highlight any comments or targets for a particular environment.

On completion of an onsite audit, if an organisation has met all the requirements the QSA will provide a Report on Compliance.



With security-assessment.com you do not just get a scan or an audit but rather the support and expertise of our whole team of information security specialists.

Our services are largely fixed price to improve planning and scoping for PCI Compliance requirements.



Security-Assessment.com

- ✓ Qualified Security Assessors
- ✓ Use Approved Scanning Tools



PCI Service Offerings

Security-Assessment.com is a certified QSA under the PCI Program. We work with you to understand your audit requirements and scope and implement a pragmatic compliance framework aligned to your enterprise security strategy and businesses strategic requirements. .

We are certified to provide you with the following mandated services.

- Quarterly Network Vulnerability Scanning.
- PCI Onsite Audits

We are also certified to provide Payment Card Application Best Practice Security Reviews which, while voluntary at the moment are sure to become the next compliance requirement.

With Security-Assessment.com you do not just get the scans and onsite audit. You get a partner that wants you to succeed. Our position is that purchasing approved products does not ensure compliance with the standard. Organisations need to be cognizant not only of how they implement the solution, but of how they "manage and maintain those system.

We see common problems with many security implementations where the emphasis is on a product or technology solution. Security is not solely about a technical solution or product, but more so on how that product and technology is integrated within a comprehensive security program involving people, policies, processes and technology. Too often companies treat information security as a technical problem and therefore apply technical solutions rather than treating information security as a **business issue**.

PCI Advisory Services

How an organisation approaches PCI compliance project is key. Doing it without expert advice can complicate the project and become a more costly exercise than what it should be. Security-Assessment.com can assist you in understanding and identifying a pragmatic and cost beneficial PCI Compliance Roadmap.

- Scope and PCI Compliance Roadmap Implementation.
- PCI Compliance Gap Assessments
- Self Assessment Questionnaire facilitation
- Business Process Reengineering

PCI Audits

The PCI DSS defines specific requirements for how applications should be developed if they process, store and transmit credit card and cardholder data. Security-Assessment.com can assist in the proactive identification of PCI application requirements that can be incorporated into the application life cycle:

- PCI Requirements Definition
- Application and Secure Coding Policies
- PCI Application and Architecture Design
- Application and Penetration Testing
- Development Team Training

PCI Mandated Audits

Security-Assessment.com is a QSA auditor and uses approved scanning tools. We work with you to understand your audit requirements and scope. We are certified to provide you with:

- Quarterly Network Vulnerability Scanning.
- PCI Onsite Audits

With security-assessment.com you do not just get a scan or an audit, but rather the support and expertise of our whole team of information security specialists.

Web Application testing

Penetration / Web Application testing should be done annually to comply with PCI. It extends the vulnerability assessment by providing tangible evidence that the environment can be compromised and to what extent. Examples of tests include;

- Gaining unauthorised access to servers or devices
- Obtaining sensitive information
- Modifying data
- Accessing another customers information and accounts
- Accessing protected functionality without valid credentials

Advise Assess Assure

- ✓ Qualified Security Assessors under the Payment Card Industry DSS.
- ✓ Endorsed Commonwealth Government of Australia supplier.
- ✓ Sit on the Attorney-Generals Critical Infrastructure Project panel.
- ✓ World leading IT Security researchers.

At Security-Assessment.com we pride ourselves on being one of the leading security research and development organisations, not just in the Asia Pacific region but around the globe.

In 2003 and 2004 we published more Microsoft security advisories than any other Asia Pacific Organisation. In 2005 and 2006 our research into Web Application Security resulted in the development of one of the worlds first webcode analysis tools. In 2005, 2006 and 2007 we published numerous advisories for serious security threats in major applications, researched and presented many world leading proof of concepts such as "Anti-Forensic Rootkits" and "Physical Attacks against Firewire" as well as presenting at various industry conferences as subject matter experts.

In 2006 Security-Assessment.com was the only external organisation from Asia Pacific, and one of five globally invited by Microsoft to present at their internal security conference, Blue Hat. This conference's goal was to assist Microsoft in better understanding how to develop more secure systems. The NY Times reported that "Security-Assessment.com is seen as a leading organisation in terms of knowledge and expertise by Microsoft.

It is our focus, expertise, experience and commitment to the industry that makes us who we are.

For more information on our research visit us at:

www.security-assessment.com

What we do

Management and Governance

- Management & Governance Reviews
- ISMS Implementation Planning
- PCI / Standards & Compliance Advice

Legal and Regulatory

- Compliance Requirements Analysis
- Compliance Requirements Register Development

Risk Assessment

- Environmental Scoping
- Risk Management Process Development
- Business Impact & Risk Assessments

Policies and Standards

- Policies & Standards Review
- Policies & Standards Development

Compliance and Awareness

- Compliance & Awareness Review
- Security Awareness Training Programs
- Secure Developer Training Programs

Security Assurance

- Vulnerability Assessments
- External and Internal Penetration Tests
- Web Application Reviews
- Source Code Inspection
- PCI Assessments & Audits
- Architecture & Controls Reviews
- Business Partner & Third Party Reviews
- Telco & VOIP security Reviews
- Wireless Network Security Reviews
- Social Engineering Reviews
- SCADA Network Security Reviews

Incident Management

- Incident Management Process Reviews
- Incident Management Business Impact Assessment
- Incident Management Plan Development
- CSIRT Support Services

Performance and Metrics

- KPI Analysis and Development