

White Paper

Payment Card Industry (PCI) Data Security Standard (DSS)

This White Paper is intended as an introductory document to help you understand the Payment Card Industry (PCI) Data Security Standard (DSS). The comments and advice are based on recent experience and reviews of the sometimes conflicting views offered and are designed to give you an insight of what the practical implications might be for your organisation. This paper is intended as an introduction to the subject and is neither exhaustive nor complete as the requirements and standards are subject to constant change.

The first question we must ask ourselves is what is the PCI DSS?

The DSS is published by the PCI Security Standards Council, collaboration between the major payment card brands, including **MasterCard, Visa, American Express and Discover**. With the rise of new technologies, from wireless networks, to on-line e-commerce systems and the ubiquitous use of these services particularly in public places like Railway stations, airports and your local Starbucks has come a dramatic increase in payment card fraud.

The Credit Card companies initially worked with online merchants to adopt security standards to protect consumer data, such as card numbers. The result is a system known as the Payment Card Industry Data Security Standard, or PCI. The PCI standard established a list of 12 detailed requirements that large merchants and service providers that handle cardholder data must have met by June 30, 2005. These requirements include strong end-user access controls and activity monitoring and logging, as well as the need to regularly test security systems and processes. Merchants that accept credit card payments now have to prove that their payment systems have the proper security measures to stop fraud and compromised data, or risk substantial fines. These standards were extended to a wider audience including Local Authorities and others who processed or received card payments at the end of 2009

The main driver for the development of the standard has been the need to reduce fraud. Forensic investigations repeatedly show that network security weaknesses and bad practice are to blame for data breaches. The standard has been developed to address the common vulnerabilities that repeatedly lead to breaches. In doing so, focus on payment card security has shifted from the finance to the IT department.

This emergence of PCI DSS is a good example of an industry developing strict self-regulation in response to not only healthy self interest but also consumer demand for greater protections from their card providers. It is also true that by taking pre-emptive action the payment card industry has in some respects avoided the situation worsening, with different countries imposing a disparate range of standards on the sector.

The case for tighter and more robust security in this area is best exemplified by looking at the case where hackers stole 40 million card details by hacking the wireless networks of retail shops.

The standard *primarily* applies to anyone storing, processing, or transmitting debit and credit card data. This brings not only merchants, but a wide range of service providers, within the scope of the standard including organisations such as ourselves specialise in the reverse logistics of IT and Telecoms equipment.

The standard is primarily being enforced by the acquiring banks – to whom merchants ultimately send their transactions to, and receive payment from.

Currently, there are many service providers who should be compliant with the standard, but are 'hidden' from the acquiring banks because they do not have a direct relationship with them for example systems Integrators who might host a retailers services or even network providers who provide the fixed or wireless networks over which the data is transmitted.

Merchants have to declare all service providers as part of their compliance validation. To back up the standard, the card brands have developed a range of penalties, and have applied them where breaches have occurred. These penalties include:

1. Repayment of all fraud committed with the compromised cards.
2. Recovery of forensic investigation costs; and
3. Other fines designed to take into account the level of compliance to the security standard at the time of the breach.

Based on fines imposed to-date, the direct losses for businesses suffering a breach are currently averaging over £100 per card for internal breaches, and even more for breaches originating within third parties.

The growth in credit and payment cards has been exponential especially if we consider that in the US in 1965; only 5 million cards were in circulation. At the end of 2009 Total credit cards in circulation in the U.S were 576.4 million (Source: Nilson Report, February 2010).

Credit and debit card fraud in the UK is estimated to cost the banks £440M in 2009 with 6.4% of card owners subjected to fraud in 2008-09 compared with 4.7% the previous year. (Source: Times, May 19th 2010). With breaches in basic data security and increased penalties imposed under the Data Protection Act for failures, it is easy to see why so much attention is being paid to data and card security.

A retailer in particular can begin to assess the potential impact of a breach of payment card data by simply multiplying the numbers above by the number of details a retailer or their service provider store, process and transmit on a daily basis. The liabilities are significant and hence the Payment Card industries desire to address the issue before the regulators impose even more draconian penalties.

Do you need to be Compliant?

The short answer is "yes". If you are processing, transmitting or storing payment card details on your network, then you must comply with the PCI DSS. Although this primarily applies to retailers or card merchants it can also apply to their service provider.

What does vary is the requirement to demonstrate compliance through the process of validation. A merchant should be in receipt of the validation requirements from their acquiring bank and if you are a service provider these requirements should be provided by the client i.e. the merchant.

Acquiring banks have to report to the card brands the level of compliance of their merchants. There is undoubtedly a variation in how hard the acquiring banks are pushing PCI DSS compliance, as they prioritise organisations according to size, and therefore liability.

Many third-party service providers were caught unawares in mid 2009 when the emerging requirements to comply with both PCI and Connecting for Health (MPfIT) requirements began to cascade down from a disparate range of clients including Local Authorities.

The scale of this particular challenge is largely unknown particularly to third party service providers, largely as a result of them being hidden from the view of the card issuing *acquiring banks*. It is only when a merchant identifies the service providers through their compliance activities, that service providers find themselves needing to take action. In this case, the merchant's own compliance usually depends on the service provider's compliance. As a consequence they will need to meet the client's requirements quickly or risk the merchant taking their business elsewhere.

Visa and MasterCard are now helping merchants choose more secure service providers by publishing the details of those who have already met the relevant requirements of the PCI DSS, and had an assessment from a Qualified Security Assessor (QSA).

Although there are a large number of organisations that need to be compliant, the method of validating that compliance does vary according to the activities you currently undertake with payment cards.

Organisations dealing with larger volumes of card details need to conduct on-site validation; with the services of a Qualified Security Assessor (QSA) they can also validate their compliance via a self-assessment questionnaire the tool developed by the PCI DSS which is available to download is particularly useful:

<https://www.pcisecuritystandards.org/education/prioritized.shtml>

Even without the need for on-site QSA assessments, the services of a QSA are recommended to help you understand the requirements of the PCI DSS, and how to apply it in your environment. One key benefit of QSAs is that they should be offering you independent advice, and not pushing you down the route of expensive vendor hardware and software 'solutions', which have limited benefits in meeting the requirements. Although a number of the vendors like Arcsight <http://www.arcsight.com/company> has useful white papers and insights.

Even if you don't have an immediate compliance requirement:

1. There may be opportunities for you to sell PCI DSS compliance services to merchants.
2. You may have some very confidential information that warrants a similar level of protection to that provided for in the PCI DSS. Rather than create a security programme from scratch, it may make sense to use the work already completed in designing the standard.

Requirements of PCI DSS – The detail

The PCI DSS has a number of objectives, broken down into twelve requirements that, in turn, are expressed in over 200 specific controls.

The PCI DSS have attempted to make the whole compliance journey a lot easier and have developed a methodology they call the Prioritized Approach and toolset. These can be found at:

<https://www.pcisecuritystandards.org/education/prioritized.shtml>

The Prioritized Approach provides guidance that will help merchants and their service providers identify how to reduce risk to card holder data as early on as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy.

The Prioritized Approach for PCI DSS 1.2 was created with input from the PCI SSC Board of Advisors, and informed by insight from real world results of data compromises shared by the assessment community. The Prioritized Approach offers guidance on how to focus PCI DSS implementation efforts in a way that expedites the security of cardholder data. It also

- Helps businesses identify highest risk targets
- Creates a common language around PCI DSS implementation efforts
- Enables merchants to demonstrate progress on compliance process to key stakeholders – banks, acquirers, QSAs, others

At the heart of the standard is the requirement to not store sensitive authentication data once the card authorisation process has been completed. This is also complemented by the requirement to protect the actual card number, usually with encryption. The hardened core data storage is then protected within a defined security perimeter, through a specific set of controls maintaining network security.

The network is also segmented, and protected, including separation of any wireless networks with firewalls. Security devices are not limited to firewalls, but also include Intrusion Detection or Intrusion Prevention, and other alerting mechanisms. These detection and alerting systems have to be backed with the rigorous reviewing of alerts and logs to ensure that incidents are not only detected, but also managed proactively and appropriately.

Remote access must use two-factor authentication, and passwords must be managed in line with specific controls, including strength, change period, and lockouts. The extensive access controls are also augmented by physical security countermeasures, including mandating the use of cameras to monitor sensitive areas. These countermeasures extend to cover physical media and documents, even though the standard is primarily concerned with electronic data security. The non-technical elements include a requirement to conduct a formal risk assessment. In addition, a range of policies and procedures are required to support the management of the controls.

The final validation process depends upon the scale of the business. Although guidance tables are available from MasterCard, Visa and American Express, the acquiring bank will advise on the specific compliance level and the associated requirements. It is important to remember that the PCI DSS applies in full, irrespective of your compliance level and validation route.

For organisations processing a larger number of transactions, they will need an annual on-site audit conducted by a Qualified Security Assessor (QSA). This must follow the standard testing procedures, and requires detailed verification of all parts of the PCI DSS.

For smaller numbers of transactions, organisations are able to complete a self-assessment questionnaire, rather than conducting an on-site audit. This is usually completed with the help of a QSA, who will be able to give independent advice to senior management before responsibility is taken for declaring compliance. Once again the most useful source of data and lists of QSA can be found on the PCI Security Standards web site.

Organisations are required to undertake penetration testing, both annually and after major system changes. In addition, they need to undertake both internal (network and application) and external quarterly vulnerability scans. The external scans must be conducted by an Authorised Scanning Vendor (ASV). In addition, at the point of validation must have evidence of a 'clean' scan.

Other areas with particular relevance to service providers and those merchants with their own IT operations include the requirement to manage a secure software development process, and correlate and analyse security logs on a daily basis. It is also worth remembering that validation is only confirmation of your compliance at a single point in time – there is a need to ensure continuous compliance to manage ongoing risk of a breach.

PCI Key Players and Roles

Card Brands

The standard is a result of collaboration by the card brands Visa, MasterCard, American Express, Discover, and JCB. Their priority is to reduce fraud losses, so that individuals and organisations make more use of their cards.

PCI Security Standards Council

They publish the relevant standards, forms, and manage the appointment and continued quality of QSAs and ASVs.

Qualified Security Assessors (QSAs)

The key advisers and assessors used by all the parties listed here. They are certified by the Council, and subjected to ongoing quality assurance audits and an annual re-certification examination.

Issuing Banks

Produce cards and offer them to consumers.

Acquiring Banks

Are the links to the merchants, taking the daily card transactions. They are tasked by the card brands to ensure merchants, and service providers are

compliant, and pass on fines and penalties to the merchants. Therefore, they don't have liability for losses. They are not experts in the standard, and have b

been known to encourage merchants to submit 'complete' assessments so that they can report compliance to the card brands.

Merchants

Anyone who takes payments using cards - The standard merchant agreement states that they have to be compliant with the PCI DSS and that they have unlimited liability for losses.

Service Providers

Handle card details or access the systems of merchants. Liability for losses to merchants is dependent upon the contract in place. This group can be as diverse as Systems Integrators, Network Providers and the Reverse Logistics provider who de-commissions and disposes of EPOS equipment.

Approved Scan Vendors (ASVs)

Certified to sell quarterly vulnerability scans.

PCI DSS and ISO 27001

As ISO 27001 is becoming the de facto standard for information security management, it is worth exploring the links with the PCI DSS. You could argue that, given the requirement to meet regulatory and contractual requirements, that the PCI DSS could integrate directly into the ISO 27001 framework. However, there are some significant differences in approach:

The ISO 27001 standard gives an organisation, within a defined management approach, a great deal of flexibility. Based on their own risk assessment, the organisation can select which of the 133 controls are appropriate for them. The PCI DSS, although requiring a risk assessment, does not give this flexibility. The 225 controls are all mandatory. The only way to avoid a control is to design an appropriate 'compensating control', and this process is often as demanding as the original.

By examining the controls closely, it can be seen that the ISO 27001 controls are deliberately not technology specific. This gives the standard a longer shelf-life, and further supports the concept that an organisation decides the appropriate security countermeasures based on its own requirements and assessment of risk.

In contrast, the PCI DSS is very specific, including dictating technologies ranging from Intrusion Detection Systems (IDS) to File Integrity Monitoring. In addition, the PCI DSS specifies standards such as password change frequency, screen saver idle time, and even a maximum time period to install security patches (something that many would argue is not necessarily 'best practice').

An organisation can apply their ISO 27001 to the scope of choice, subject to certification body approval. The PCI DSS scope is dictated by the extent of your payment card transaction processes, although as we shall see in the next section, you can limit this to reduce the requirements.

PCI DSS Compliance

The PCI DSS is only concerned with a small part of your information security, namely the confidentiality of card data. While the ISO 27001 takes a much broader view, in ensuring not only confidentiality, but also integrity and availability of information and extends beyond electronic data to include all forms of information. This is illustrated by the approach to backups.

The ISO 27001 requires a policy on backups, with defined coverage and testing to ensure availability. In contrast the PCI DSS process positively discourages backing up, other than keeping security audit logs for a minimum of 12 months.

The presence of card data on multiple backup media is not helpful in keeping them confidential. This lack of interest in maintaining systems is also demonstrated by the fact that the PCI DSS contains no requirements for Business Continuity or Disaster Recovery - the focus is only on maintaining confidentiality.

Only UKAS accredited certification bodies should award certificates for ISO 27001, although we still meet non-UKAS certifications with variations in quality that you would expect. However, the PCI standard allows the same QSA to consult, guide and help an organisation reach a level of compliance, and then conduct the validation audit. This would appear to be weakness. However, the QSA's organisation has to go through a rigorous application process and, perhaps more significantly, their final sign-off carries with it a degree of responsibility, and liability, that should ensure an objective approach.

Strategy and Common Pitfalls

The approach an organisation takes to securing compliance to the PCI DSS can greatly influence the time and resources required. Although a demanding standard, you can ensure the process is as efficient as possible, and target your efforts to meet the requirements. The intent of the standard is to help you achieve a reasonable level of security for the activities you conduct, and certainly not to force unnecessary investments.

Although it is good practice to engage the services of a Qualified Security Assessor (QSA), the first mistake people often make is to commission a large-scale gap analysis of their systems. This is likely to show massive gaps against the PCI DSS, and give you a near impossible action list of new technology and processes required to secure compliance. Therefore a more considered approach is required.

If you are a merchant then you should review your current payment card data processes, and the associated relationship(s) with your acquiring bank(s). It may be appropriate to consolidate some of these to reduce your PCI DSS requirements.

Your acquiring bank is required to communicate your compliance level to the standard, and the form that your final validation will take.

It is therefore worth entering into a dialogue with them to demonstrate that you are committed to the process. This can help when you need their confirmation of how you intend to interpret a given requirement.

The next stage is to produce detailed transaction mapping of your current systems, to identify all payment card data stores and transmission paths. In this process you will also need to identify third-party service providers. It is important that you identify third-parties at an early stage, as for merchants the agreement with your acquiring bank gives you responsibility for costs associated with a compromise on their part. It is also worth reviewing contractual arrangements between you and your service providers to ensure suitable liability clauses are included.

It is recommended that, having established your service providers PCI DSS compliance status (which will largely be led by your processes and requirements set out in their original engagement), you inform your acquiring bank of their involvement. In many cases, third-party service providers are hidden from the acquiring banks, and given your likely financial liability it is not in your interest to let them remain so.

It is worth remembering that the most recent statistics show that merchant (and this includes unlikely bodies like Local Authorities) losses are likely to be more if the breach originates within one of your third-party suppliers. You should also examine your contractual terms with these suppliers to see if, should the worst happen, you have any grounds to recover your fines. The acquiring banks will fine you, not your suppliers.

By identifying non-compliant third-parties at the early stages of your compliance programme, you give them time to meet the requirements. Alternatively, you may wish to seek alternative suppliers of the services in question, as you currently cannot achieve compliance without the compliance of all your third-party service providers. However it is incumbent on you as the Merchant to ensure your service providers have a clear understanding of your compliance requirements.

The next and probably the most crucial steps are to ensure compliance with PCI/DSS Requirement 3:

Protect stored cardholder data. The reasons you need to do this at the earliest opportunity are threefold:

1. If you are storing authentication details not permitted by the DSS, or not encrypting data as required you greatly increase the potential losses incurred if the data is compromised.
2. Any changes to data storage and encryption will often necessitate modification to system code, and this can be time consuming.
3. You will probably want to purge systems of data to limit the scope of compliance.

It is worth mentioning at this point that many product vendors, as always, are offering very solutions to the requirements, and making promises of PCI DSS compliance. However as always in our experience before any investment is considered there are often more cost-effective routes to compliance.

Once you fully understand the scope of your PCI DSS related systems, you can then plan the crucial stage of network segmentation. This is the best route to limit your compliance requirements and keep the project under control. It is worth remembering that many vendors will not mention this, as it also limits their opportunity to sell you 'solutions'. However it should be a service that most providers should offer certainly as an initial audit.

By limiting the scope, through appropriate network segmentation, you can make the whole compliance project much more manageable. Most network providers will offer expert advice and audits as they have a vested interest in ensuring they do everything to not only support your compliance but to ensure they retain your business.

It is at this point, that a gap analysis makes much more sense, mapping the detailed standard requirements to your reduced compliance scope and giving you a detailed, and realistic, remediation plan.

Where Next?

The PCI DSS is being driven by increasing fraud activity, and the targeting of organisations handling payment card data. The requirements are detailed and, for many organisations, challenging.

This White Paper has been written in response to customer enquiries and whilst not intended to provide chapter and verse on the subject should provide sufficient insight to allow better informed decisions. It is intended to inform and help clarify the myriad of acronyms that are inevitable whenever security emerges as a topic.

There are numerous industry bodies and vendor who can provide consultancy and solutions. The first place we recommend any client starts the process is by talking to their network services provider and reviewing the excellent material available at www.pcisecuritystandards.org

It is also worth investigating what some of the major vendors are up to Arcsight and RSA are two who have a track record in this space:

Arcsight <http://www.arcsight.com/company> and RSA the security Division of EMC are just two who are specialist in this area. <http://www.rsa.com> .