

# » Using ISO 27001 for PCI DSS Compliance«

A white paper by Steve Wright,  
Siemens Insight Consulting



The Payment Card Industry Data Security Standard (PCI DSS) isn't dramatically different to the requirements of the best practice security standard - ISO 27001, except that PCI doesn't mention any of the prerequisites required for a management framework, e.g. management commitment, scope definition, security awareness training, ongoing improvement plans, whereas ISO 27001 omits a lot of the detail around how controls are actually implemented. So therefore, one could be forgiven for believing that MasterCard and Visa assumed PCI would contain additional security requirements to sit on top of an already established Information Security Management System (ISMS).

There is no getting away from the fact that this is good news for industry as a whole. Any new baseline security standard that helps measure the security of systems is good news. For example, making sure that firewalls are only passing traffic on accepted and approved ports, ensuring that servers are running only those services that really need to be live and validating those databases aren't configured with vendor supplied defaults.

The problem is, like with any baseline standard, it is only as good as the last review; and herein lays a dilemma. ISO 27001 has deliberately moved away from specifying or dictating too many detailed controls (133 in ISO 27001, but over 200 in PCI), as it did not want it to become a simple tick box exercise. ISO 27001 stipulates that an organisation should ensure any control to be implemented should reflect the level of risk (or vulnerability), that could cause unnecessary pain should it not be addressed.

PCI does refer to conducting a formal risk assessment (see section 12.1.2 of the standard), but how flexible would a certified third-party auditor be during the audits?

Would he /she agree with the organisation that the risks acceptable to one organisation were deemed unacceptable to another (depending upon the risk appetite of the organisations)?

PCI, as it is almost universally known, was originally developed by MasterCard and Visa through an alignment of security requirements contained in the MasterCard Site Data Protection Plan (SDP) and two Visa programs, the Cardholder Information Security Plan (CISP) and the international Account Information Security (AIS). In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. Concurrent with the announcement, the council released version 1.1 of the PCI standard. Since then it has rapidly become the 'de-facto' standard within the card industry for both merchant and service provider.

While the newly-established PCI Security Standards Council manages the underlying data security standard, compliance requirements are set independently by individual payment card brands. While requirements vary between card networks, MasterCard's Site Data Protection Plan and Visa's Cardholder Information Security Program are representative. They stipulate separate compliance validation requirements for merchants and service providers, which vary depending on the size of the company and its transaction / business throughout.

PCI DSS is based on established best practice for securing data (such as ISO 27001) and applies to any parties involved with the transfer or processing of credit card data.

Its purpose is to ensure that confidential cardholder account data is always secure and comprises 12 key requirements:

### **Build and maintain a secure network**

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

### **Protect cardholder data**

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

### **Maintain a vulnerability management program**

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

### **Implement strong access control measures**

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

### **Regularly monitor and test networks**

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

### **Maintain an information security policy**

- Requirement 12: Maintain a policy that addresses information security

In order to fully comply with the standard, every organisation that the standard applies to must implement all of the controls to the target environment and annually audit the effectiveness of the controls in place.

### **PCI validation requirements & ISO 27001 compliance requirements**

Both ISO 27001 and PCI require the organisation to ensure that a formal validation and compliance (audit) structure is in place and that validation requirements (including self audits and vulnerability scans) are undertaken on a regular basis and results are fed into a management system for ongoing review and improvement (e.g. PCI validation requirements are based on number of transactions - the more transactions an organisation handles, the greater the quantity and detail of audits that are required).

The number of validation audits includes:

- **Annual on-site security audits** - MasterCard and Visa require the largest merchants (level 1) and service providers (levels 1 and 2) to have a yearly on-site compliance assessment performed by a certified third-party auditor, which is similar to an ISO 27001 certification programme
- **PCI annual self-assessment questionnaire** - In lieu of an on-site audit, smaller merchants and service providers are required to complete a self-assessment questionnaire to document their security status. Again this is similar to ISO 27001, as there should be a formal structure of scheduled audits that enables early identification of 'weak spots' and should feed into an existing 'enterprise risk structure' that enables the organisation to fulfil corporate governance requirements, such as Basel II, SOX, Combined Code, Revised Guidance, OGC, OECD and FSA
- **Quarterly external network scans** - All merchants and service providers are required to have external network security scans performed quarterly by a certified third-party vendor. Scan requirements are rigorous: all 65,535 ports must be scanned, all

vulnerabilities detected of level 3-5 severity must be remedied, and two reports must be issued a technical report that details all vulnerabilities detected with solutions for remediation, and an executive summary report with a PCI approved compliance statement suitable for submission to acquiring banks for validation.

One important thing to note is that PCI have created security audit procedures (a tick box / checklist document) that provides information on the requirements for technical PCI compliance and also provides details on the expected content that should form part of the annual submission report - the 'report for compliance or executive summary report'. To assist service providers or merchants in this compliance process an 'accreditation' scheme has been established. This has been designed to allow pre-approved PCI security and audit organisations to offer 'Qualified Security Assessor' (i.e. Auditor of system) services or Approved Security Vendor (i.e. Penetration tester), or both.

These services will appeal to the many service providers or merchants that need to comply on all levels with PCI DSS, but ultimately, every service provider or merchant will have the option of who they choose to work with to verify they meet all the technical requirements of PCI DSS.

#### PCI DSS Validation Enforcement Table

While PCI DSS non-compliance penalties also vary among major credit card networks, they can be substantial and perhaps more worryingly, they can represent a major embarrassment or worse, lead to reputation damage, which is difficult to quantify.

Participating companies can be barred from processing credit card transactions, higher processing fees can be applied, and in the event of a serious security breach, fines of up to £250,000 can be levied for each instance of non-compliance. Since compliance validation requirements and enforcement measures are subject to change,

merchants and service providers need to closely monitor the requirements of all card networks in which they participate.

#### PCI and ISO 27001 - the comparisons

In contrast to the PCI framework, the ISO 27001 standard is more flexible in terms of scope, controls, compliance and enforcement. As an internationally recognised security standard, ISO 27001 is designed to apply to a wide variety of organisations across numerous industries. It is regarded as the de-facto information security standard by many organisations where information security is a strict requirement; although compliance is voluntary. Many organisations that choose to certify to the standard often do so for purposes of due diligence or partner confidence.

When properly applied ISO 27001 is based around a flow of information, which makes up what the standard defines as a system. The organisation defines the systems to be certified and sets up an Information Security Management System (ISMS) around the relevant area of business, which is then defined as the scope.

Subsequently the organisation fully documents the scope, creates a detailed asset inventory and performs a formal risk assessment on those assets. The results of the risk assessment lead the organisation to the control clauses of the standard and they choose those that best address the risks to the environment. The selected controls are then documented in its Statement of Applicability (SOA) and mapped back to the risk assessment.

	Level	Criteria	On-site Security Audit	Self Assessment Questionnaire	Network Scan
SERVICE PROVIDER	1	All processors and all payment Gateways	Required Annually		Required Quarterly
	2	Any service provider that is not in Level 1 and stores, processes or transmits more than 1 million accounts / transactions annually	Required Annually		Required Quarterly
	3	Any service provider that is not in Level 1 and stores, processes or transmits less than 1 million accounts / transactions annually		Required Annually	Required Quarterly
MERCHANT	1	Any merchant, regardless of acceptance channel, processing more than 6 million transactions per year – Any merchant that suffered a security breach, resulting in an account compromise	Required Annually		Required Quarterly
	2	Any merchant processing between 150,000 to 6 million transactions per year		Required Annually	Required Quarterly
	3	Any merchant processing between 20,000 to 150,000 transactions per year		Required Annually	Required Quarterly
	4	All other merchants not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually	Required Quarterly

Figure 1—PCI DSS Validation Enforcement Table

PCI DSS requirements or controls are mandatory - if an organisation wants to comply with PCI DSS then it must comply with every requirement laid out in the standard. In contrast, ISO 27001 controls are suggested controls, and each organisation has the flexibility to decide which controls it wants to implement dependent upon the risk appetite of the organisation.

Compared to ISO 27001 requirements, PCI DSS controls are much more specific. This granularity should, in theory, make auditing of PCI DSS easier than ISO 27001 but conversely, the specific controls required for PCI DSS remove a certain amount of flexibility and could make compliance more difficult to achieve.

Analysis of the two standards show that there are gaps between PCI DSS and ISO 27001, but these gaps do not mean that an ISO 27001 information security programme is unable to meet PCI DSS requirements. What they do show is that whilst ISO 27001 may have a similar type of control on the PCI related system, the control is unlikely to have the granularity required by PCI DSS.

Characteristic	PCI DSS	ISO 27001
Implementation of controls	Mandatory	Based on risk assessment
Degree of granularity	High	Low
Degree of flexibility	Low	High
Management of Systems	Low contribution	Considerable contribution

**Figure 2—PCI DSS & ISO 27001 Characteristics Table**

Detailed planning when considering ISO 27001 certification could allow an organisation to meet both standards with a single implementation effort.

The two standards have very different compliance requirements. Generally, ISO 27001 provides guidance to an organisation in implementing and managing an information security programme and management system, whereas PCI DSS focuses on specific components of the implementation and status of 'applicable' controls.

Most organisations who have implemented an ISO 27001 Information Security Management System do not have to invite external third parties to validate that they are operating within the realms of a compliant ISMS.



However, anyone claiming to be compliant to ISO 27001 now has to address all the requirements of the Clauses 4-8 found in ISO 27001, which define the Information Security Management System: i.e. risk assessment & methodology, audit schedule, effective measurements, etc.

This effectively means that ISO 27001 is now more focused on implementing controls based on risk, and ensuring that monitoring and improving the risks facing the business are improved, as opposed to simply stipulating which of these were 'not applicable' under the old standard BS 7799, or ISO 17799.

Therefore, irrespective of whether they are claiming to be compliant or certificated to ISO 27001 (ISO 17799) this is now a mandatory requirement and therefore aligns itself more to PCI DSS.

In addition, whilst ISO 27001 is more focused on control objectives, PCI DSS has a blend of control objectives and controls specific to the standard. However, most PCI DSS requirements are covered by ISO 27001 - only lacking specific implementation details in certain areas. Using ISO 27001 as a means to meet compliance targets could be regarded as an appropriate methodology to meet requirements of the PCI framework. However, in order to attain PCI DSS compliance an organisation's ISMS must address the specific granular requirements and follow the PCI requirements exactly.

Once again, ISO 27001 (A.15.3.1) overlaps with the well defined audit regime for PCI DSS, with ISO 27001 'Control A.15.2.2 - Technical compliance checking' specifically requiring annual penetration tests are conducted. In contrast to PCI DSS, additional mandatory requirements within ISO 27001 'Compliance Section' (A.15) also require organisations to ensure ongoing compliance with appropriate legislative, regulative and contractual requirements. This effectively means that two security standards complement each other when it comes to audit and compliance.

If a properly developed and implemented ISMS is in place with full documentation and working processes, it can result in a comprehensive security management approach and will give visibility to the fact that the controls are in place and are being managed and measured. Provided the ISO 27001 methodology is implemented correctly (clause sections) with the emphasis on specific details pertinent to both standards, this approach should meet all the relevant regulatory and legal requirements and prepare any organisation for future compliance and regulatory challenges.

This however, confirms the view that less focus is given to 'management aspects' or, put another way, less time is spent on ensuring the ongoing improvement and management elements of a ISO 27001 compliant ISMS (as you might expect) are required.

PCI DSS	ISO 27001 relationship										
	A 5	A 6	A 7	A 8	A 9	A 10	A 11	A 12	A 13	A 14	A 15
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: Use and regularly update anti-virus software						✓	✓				
6: Develop and maintain secure systems and applications						✓	✓	✓			✓
7: Restrict access to cardholder data by business need-to-know							✓				
8: Assign a unique ID to each person with computer access							✓				
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	✓	✓	✓	✓		✓	✓	✓	✓	✓	

**Figure 3 - PCI DSS & ISO 27001 Relationship Matrix**

From the above illustration you can see that most of the PCI controls focus around the three ISO 27001 sections (highlighted in green), which address the technical elements of data security:

A.10 - Communications and operations management, dealing with all aspect of change control, virus, back up and monitoring;

A.11 - Access control, dealing with all aspects of user ID management, network access, operating systems and remote working;

and finally

A.12 - Information systems acquisition, development and maintenance, dealing with all aspects of technical design specifications, input / output data validation, patch management, cryptography and application development generally.

# Using ISO 27001 for PCI DSS Compliance

## Summary

Whilst these important technical sections are dealt with more than adequately within PCI DSS, the 'mandatory' requirements of ISO 27001 ISMS, namely the clause sections and A.5 - Security Policy, A6 - Security Organisation (Third parties), A13 - Security Incident Management / Crisis Management,

A14 - Business Continuity and Disaster Recovery (BS 25999) and A.15 - Audit & Compliance are only referred to briefly within PCI DSS. However, at the same time, this does once again demonstrate the close relationship between the two standards and therefore enforces the message that ISO 27001 can help an organisation achieve and manage a PCI DSS environment and also underlines the original point; that it appears that PCI DSS was designed to simply fit onto an existing ISO 27001 ISMS.

In conclusion, PCI DSS is a great technical standard, but still needs an Information Security Management System to manage it.



## Authors biography

Steve Wright is a Senior Consultant at Siemens Insight Consulting providing professional advice in relation to information security, technology and management to meet BS 7799, ISO 27001, ITIL, ISO 20000, PAS 56, PAS 99, PCI DSS, ISO 13335 and works within legal and regulatory frameworks such as Basel II, SOX and Combined Code requirements. In addition, Steve is accustomed to implementing risk best practices such as enterprise risk management frameworks and conducting risk assessments, using tools such as CRAMM.

Steve is currently project managing many implementations of ISO 27001 ISMS systems, both virtually and physically, from initiation through to final delivery, to meet certification requirements of ISO 27001, ISO 9001 and ISO 20000 in both financial, private and public service sectors, three of which have recently achieved Certification to ISO/IEC 27001:2005 in late 2006 alone.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Enterprise Communications Limited and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CESA Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against ISO 27001 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at [www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)  
Siemens Insight Consulting  
Tel: +44 (0)1932 241000  
Fax: +44 (0)1932 236868

[www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)