

## The PCI Standard (actions required by organisations) and How ISO 27001 Aids Compliance

### Background to the PCI standard

Following a series of high profile security breaches, credit card users are putting payment processors and merchants under pressure the confidentiality and security of personal and transactional data. *Visa* and *Mastercard* responded with the PCI standard which has been formally endorsed by Amex and the Diners club.

The Data Security Standard introduced will help to ensure that transactions are conducted in a secure manner, and the all 'merchants' meet minimum security standards that are verified by regular penetration testing.

The current version is 1.1 that was issued in September 2006 and apart from the 12 requirements laid down – see below; it calls for organisations to have 'Compensating Controls' in place these controls are mainly those contained under ISO 27002 the best practice standard for information security.

### Requirements

The PCI data security standard (DSS) is based on established best practice for securing data and applies to any parties involved with the transfer or processing of credit card data, the standard is made up of 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 parameter

#### 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



#### Who does the standard specifically it apply to?

Compliance applies to your organisation if it accepts stores or processes payment cards. This includes. resellers, software application providers, acquirers, payment service providers, card processing bureau, data storage entities, web hosting providers, shopping cart providers, miscellaneous third party agents, software vendors.

If your organisation is included, it will be classed within the various levels of the PCI DSS:

#### For merchants:

Merchant Level	Criteria	Compliance Requirements
<b>Level 1</b>	> 6m transactions pa	Annual onsite audit Quarterly network security scan
<b>Level 2</b>	1 -6m transactions pa	Annual self assessment questionnaire Quarterly network security scan
<b>Level 3</b>	20k to 1m e-commerce transactions pa	Annual self assessment questionnaire Quarterly network security scan
<b>Level 4</b>	Up to 20k e-commerce transactions	Annual self assessment questionnaire Quarterly network security scan

#### For payment service providers:

Service Provider Level	Criteria	Compliance Requirements
<b>Level 1</b>	All payment gateways	Annual onsite audit Quarterly network security scan
<b>Level 2</b>	Merchants processing 1 – 6m transactions pa	Annual onsite audit Quarterly network security scan
<b>Level 3</b>	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1m V/MC accounts/transactions pa	Annual Self-Assessment Questionnaire Quarterly network security scan

#### Why Comply?

- It demonstrates to customers that you take security seriously and have effective controls
- Complying provides competitive edge in protecting your reputation and brand and
- Provides regulators with assurance that processes are adequately controlled
- It will ensure Exemption from fines, if appropriate controls and actions are put in place



## How Sapphire Can Help Aid Compliance

Sapphire has developed the following phased programme of work:

### 1. Scope of Compliance

We identify the steps required for compliance based on 'the level of compliance appropriate to you' (transactions volumes etc see charts for merchants/payment service providers above)

### 2. Benchmarking Review

Sapphire will assess your current technical and procedural controls against the standard and develop a tailored action plan.

### 3. Security Improvement Programme

Sapphire will develop a suitable action plan to address the 'gaps' identified in the *Benchmarking Review* this programme is a combination of quick wins and medium term tasks.

### 4. Audit & Network Scan

We will conduct a mock compliance and certification audit including the required network penetration scans through a partnered approved scanning vendor.

## Sapphire Credentials

Sapphire consultants are Information Security Management experts who have conducted information security benchmarking reviews for clients for over a decade. Sapphire has an extensive database portfolio of security improvement templates and work closely with the PCI standard developments.

Sapphire consultants hold all the required qualifications to assist in PCI compliance work namely CHECK qualified penetration tester and CLAS consultants, ISO 27001 IRCA certified auditors with respected IS Management professionals in CISM, CISA and CISSP.

## The Relationship between PCI and the ISO27001 Security Standard

ISO 27001 is the global certification standard on Information Security Management whereby an organisation can set up an effective Information Security Framework for 'Business Resilience'.

The PCI DSS Standard is the Payment Card Industry's Security requirements (12) Version 1.1 (Sept06). This revision discusses 'Compensating Controls' which cover many of the ISO27001 requirements, the overlap between the two standards are outlined below.

The PCI standard is primarily concerned with an organisation having an adequate Information Security Regime that focuses on an IS Policy and appropriate ICT Security Controls, namely ISO27001 Requirements sections 1, 5-8.

When you analyse how to meet each PCI requirement, especially No.12 'Maintain an IS Policy', it asks the organisation to meet 4 additional requirements shown under ISO27001 (No 2, 4, 9, & 11).



ISO 27001 Requirements	PCI Requirements
1. IS Policy	12. Maintain an IS Policy <sup>1</sup>
2. Organising IS	
3. Asset Management	
4. Human Resources Security	
5. Physical/ Environmental Security	9. Restrict physical access to cardholder data
6. Communications/Operations Management	1. Install & maintain a firewall configuration to protect cardholder data 3. Protect stored cardholder data; 10. Track & monitor all access to network resources & cardholder data
7. Access Control	2. Do not use vendor-supplied defaults for system passwords & other security parameters; 7. Restrict access to cardholder data by business need to know; 8. Assign a unique ID to each person with computer access
8. System Acquisition/ Development/ & Maintenance	4. Encrypt transmission of cardholder data across open, public networks; 5. Use & regularly update anti-virus software; 6. Develop & maintain secure systems & applications; 11. Regularly test security systems & processes
9. IS Incident Management	
10. Business Continuity Management	
11. Compliance	

<sup>1</sup> 1. To meet this requirement, requires addressing the following 27001 requirements:-  
2. Organising IS; 4. Human Resources Security; 9. IS Incident Management; and 11. Compliance

Therefore addressing the PCI Standard within an ISO27001 framework is not only desirable but essential.

Below is the process that Sapphires consultants take when implementing ISO 27001.

### Sapphires ISO 27001 Consultancy Service

Sapphire provides technical consultancy, information security products and systems. Sapphires consultants specialise in **ISO 27001**, an International Information Security Standard and ISO 27002 which gives comprehensive guidance on best practice methods for managing risks to information within an organisation. Sapphires consultants have extensive experience working with both public and private sectors assisting with improving their information security measures. Sapphire can assist organisations in the development of robust information security management systems that will:

- Objectively identify and manage risks to information;
- Progress towards organisational security maturity;
- Satisfy Corporate Governance, customers, statutory and insurance requirements.



Sapphire offers a modular stage-wise programme of consultancy services designed to assure the confidentiality, integrity and availability of your information and assets. An organisation can decide which of them it needs and Sapphire's degree of involvement. Sapphire's methodology is based on ISO 27002 (ISO 17799:2005) 'Information Security Management'. Compliance to this standard is becoming an increasing requirement from customers and the government.

Sapphires stage-wise programme consists of four main phases:

- Phase 1 - Security Improvement Plan
- Phase 2 - Security Management System
- Phase 3 - Internal Audit
- Phase 4 - Review and Assessments

Compliance to ISO 27002 (ISO 17799:2005) provides:

- A common basis for developing organisational security standards;
- An effective security management practice;
- Confidence in inter-organisational dealings.

### Sapphire Strategic Support Agreement

Sapphire realises that the number of organisations that allow for a contingency amount in their Information Security budget is small. Sapphire addressed the needs of their clients and realised the importance of having a contingency plan. Should it be a major security incident or perhaps the implementation of a new product or solution, having a strategic agreement already in place will give you peace of mind, as well as ensuring you are prepared for any eventuality.

With an **SSA**, you can rest assured that Sapphire will become the middleman to make certain your solutions work together and you get the best kind of protection. What in effect is being presented to the client in the form of a SSA is a single source for all their information security requirements, with added bonus of our organisations full certification to ISO27001, the global standard for information security.

The provision of Strategic Support enables our clients to ensure that their security knowledge, systems, technical security and processes are maintained at the highest level. The support agreement can include:

1. Computer Forensics and Data Recovery
2. PCI Compliance Consultancy
3. ISO 27001 Security Audit Consultancy
4. Penetration Testing
5. Regular Security Reviews and Health-checks
6. Education and Training
7. Technical Services
8. Access to the Sapphire Helpdesk

#### Need Further Guidance?

Please contact Sapphire on **01642 702100** and ask to speak to one of our business consultants

