

PCI DSS compliance — meeting the demands

*Cian Blackwell,
Partner, and Mark
Gahan, Manager, of
Business Risk Services
at Grant Thornton,
outline payment card
industry requirements,
and advise on how your
organisation can be
compliant*

PCI DSS stands for Payment Card Industry Data Security Standard, a name that provides a clear indication of its purpose. It is a worldwide information security standard created by the Payment Card Industry Security Standards Council ('PCI SSC') and it has its origins in five separate frameworks from five different card issuers: Visa Card Information Security Program; MasterCard Site Data Protection; American Express Data Security Operating Policy; Discover Information and Compliance; and JCB Data Security Program.

The goals of each framework were broadly similar and focused on reducing the occurrence of credit card compromises amongst e-commerce web sites, acquiring organisations and merchants, and on creating an extra level of protection for the five card issuers by ensuring that merchants met minimum levels of security when they stored, processed and transmitted cardholder data.

On 15th December 2004 the PCI SSC was formed, and the card issuers amalgamated the five different frameworks to form the basis for PCI DSS, version 1.0. This has since undergone minor revisions, to version 1.1 in September 2006, and version 1.2 in October 2008. These updates have not changed requirements, merely enhanced clarity and addressed evolving risks and threats, for example wireless standards.

The PCI SSC acts as a standard-setting body and a forum, and membership is open to those directly and indirectly involved in payment processing, including payment card issuers, acquiring banks, merchants, outsourced service providers, and hardware and software vendors.

Compliance with the standards is a contractual requirement imposed on all acquiring banks by the card issuers. The acquiring banks in turn impose the requirements on merchants and so on, to include all organisations that store, process or transmit cardholder data.

One of the principal concepts in PCI DSS compliance is that of 'requirements'. Meeting the 12 basic requirements is necessary to attain PCI DSS compliance.

The requirements can be grouped under six headings:

Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data; and
- Do not use vendor-supplied defaults for system passwords and other security parameters.

Protecting cardholder data

- Protect stored cardholder data; and
- Encrypt transmission of cardholder data across open, public networks.

Maintain a vulnerability management program

- Use and regularly update antivirus software; and
- Develop and maintain secure systems and applications.

Implement strong access control measures

- Restrict access to cardholder data by business on a need-to-know basis;
- Assign a unique ID to each person with computer access; and
- Restrict physical access to cardholder data.

Regular monitoring and testing of networks

- Track and monitor all access to network resources and cardholder data; and
- Regularly test security systems and processes

Maintain a policy that addresses information security

- Maintain a policy that addresses information security.

The second principal concept in PCI DSS compliance is that of 'levels.' Merchants and service providers are all classified into levels; four levels for merchants and three for service providers. What level an organisation falls into is proportional to the volume of transactions processed, and thus

roughly proportional to the potential impact of their cardholder data being compromised.

Regardless of the level into which a service provider or merchant falls, they are still required to comply with the 12 basic requirements. Rather than affecting an organisation's compliance requirements, the levels are instead used to determine compliance validation requirements for merchants and service providers. Therefore levels affect how often an organisation is audited to verify its compliance, but do not affect the compliance requirements themselves.

For example, the providers and merchants in the highest risk category, level 1, must meet the standards, conduct and pass an annual penetration test, conduct quarterly scans, and complete and pass an annual audit using external auditors. For level 2 and 3 merchants, an annual self-assessment is sufficient in place of the external audit, but must be approved by a qualified security assessor ('QSA'). For level 4 merchants, all requirements, except meeting the standards, are optional, but even at this level, breaches of security or other data compromises will result in the merchant immediately being moved to level 1.

PCI SSC is a standards-setting body; it manages the DSS but does not enforce them or specify sanctions for non-compliance. Individual card issuers are responsible for setting sanctions, which include fines and, in extreme cases, prohibiting organisations from processing the issuer's card data.

If a card issuer has an arrangement with the acquirer rather than the merchant, the acquirer will be held responsible for security breaches within any of the merchants under its remit. Acquirers will therefore seek to pass on these fines and penalties to the relevant merchant or service provider.

Fines can rapidly reach very high levels — for a merchant that was

responsible for 10,000 cards being compromised, fines, penalties and reimbursements could potentially comprise fines of €5 per card, investigation costs of €30,000, an average fraud of €500 per card, card replacement costs of €20 per card and €30 per card in chargeback fees, totalling over €5 million.

fines and penalties, as you have taken all reasonable steps to ensure that credit card data which you are responsible for is protected and secure. Listed below are six suggestions which an organisation could use, not only to reduce the risk and the complexity of the PCI validation, but to improve overall assurance levels and manage information security risk.

PCI DSS levels — merchants	
Level	Criteria
1	<p>Merchants processing more than 6 million transactions per year</p> <p>All third party processors ('TPPs') processing data on behalf of level 1, 2, or 3 merchants</p> <p>All data storage entities ('DSEs') storing data on behalf of level 1, 2, or 3 merchants</p> <p>All merchants, TPPs and DSEs whose card data has been compromised</p>
2	Merchant processing between 1 and 6 million transactions per year
3	Merchants (other than those at level 1 or 2) with more than 20,000 e-commerce transactions per year
4	All other merchants

PCI DSS levels—service providers	
Level	Criteria
1	All processors and payment gateways
2	Any service provider, other than those at level 1, which stores, processes or transmits more than 1 million transactions per year
3	All other service providers

Six activities to achieve and improve compliance

For most organisations, compliance is a delicate balance between the investment required to achieve and maintain compliance, and the potential costs of non-compliance — not just fines but the cost of being unable to process card data. If you have been validated as compliant with the PCI DSS, you have a 'safe harbour' from

1. Understand your compliance requirements

The most fundamental step in taking control of compliance requirements is obviously to understand what is required of your organisation. PCI DSS is unlikely to be the only compliance requirement in an organisation, and compliance requirements include regulations and guidance as diverse as the Combined Code, Sarbanes-Oxley, financial regulations, and controls required to satisfy SAS 70 audit requirements. Understanding all of these requirements, and where they overlap, provides an opportunity to consolidate controls for the sake of efficiency.

2. Perform a risk assessment

Performing a risk assessment is the next critical step. During this exercise, it is not difficult to expand the scope from focusing just on PCI compliance risk to focusing on security risks in general. By conducting a high-level IT risk assessment, an organisation should be able to identify where card data are located, how data are accessed, and the general IT security controls in place.

The risk assessment can then be mapped to the PCI data security standards to assess how well compliance is being met and determine the gaps. During this exercise it is important to think like a "bad guy", and cover every likely vulnerability. While it is unlikely that a criminal will force his way in the front door brandishing a gun, he may consider gaining access to an organisation by posing as

a cleaner or by “tailgating” legitimate users through swipe card or other security controls. Every potential opportunity for criminal gain is a risk that must be addressed.

3. Understand how your controls mitigate your risks

With the risk assessment complete, you should understand what controls your organisation has in place to mitigate risks, both compliance risk and general security risk. These risks should be mapped to controls using a risk and control matrix (‘RCM’). An RCM is essential to ensure that all risks are appropriately addressed by controls, and can highlight opportunities to remove controls that are not mitigating risk, resulting in a more efficient control framework. In effect, the RCM should facilitate a balance between the efficiency and the effectiveness of controls.

4. Document your controls

Documenting controls is essential, but overlooked by many organisations. This is frequently justified using arguments such as “everyone knows what the process is”, but this is rarely true. Over time, numerous interpretations of the most appropriate way to perform any control or process will arise. Furthermore, in common situations where a control is operated or managed by just one person, the organisation will become dependent on that person and an unforeseen absence will increase control and security risk. It is useful to refer to an IT maturity model and assess the level of sophistication of your control framework. The Control Objectives for Information and related Technology, or ‘COBIT’ framework, incorporates one of the more popular IT maturity models for measuring the effectiveness and quality of processes and controls.

The general attributes used to measure the effectiveness of controls, including security processes, can be defined by five levels (see table). This maturity scale provides a measurement and comparison of how

effective the controls are in an organisation. Aside from the benefits described above, the minimum acceptable level for PCI DSS compliance is that the controls must be documented and implemented, i.e. at level 2.

5. Compartmentalise and reduce scope

One approach to tackling PCI DSS

COBIT Control Maturity Mode	
Level	Attribute
0	Control is not documented—i.e. any controls are likely to be ad-hoc and informal
1	Control is documented—i.e. there is a standard process, but it may not be in place
2	Control is consistently applied—i.e. it has been implemented
3	Control is consistently applied and continuously working—i.e. controls have been tested
4	Control is monitored—i.e. process improvement techniques are used and controls are efficient

compliance is to reduce the scope and compartmentalise your IT environment so that the controls required to gain compliance only apply to a subset of your overall IT environment. This type of isolation can be very cost effective for some organisations, but there may be drawbacks.

The downside of compartmentalisation is that you may end up with one highly controlled area and other parts of the environment having much weaker controls. While this may not impact on your PCI assessment it could result in security vulnerabilities elsewhere which could leave your organisation with equal if not more risk in other parts of your organisation. Depending on the nature and size of your organisation it may be better to implement consistent controls in all areas, regardless

of what may be dictated by compliance requirements.

6. Ensure vendors and third parties accept appropriate responsibility

A PCI DSS compliant organisation will have numerous IT systems, and whilst some applications may be developed in-house, most organisations will procure their systems from an external vendor. This should result in a sharing of the compliance burden, with the onus on vendors to demonstrate that their systems are compliant with PCI DSS. A compliant system should not store unencrypted credit card numbers or magnetic stripe data, and data should be masked, truncated or encrypted, never in plain text.

Alternatively, merchants may be able to outsource payment processing to a specialist third party, so that all credit card details reside with the service provider, and the merchant no longer has to manage the data, potentially avoiding compliance requirements. This is only effective if the service provider’s controls are adequate, not just for PCI, but to enable mitigation of all of the risks that outsourcing can present. Requiring the service provider to undergo a SAS 70 or similar periodic audit report is likely to be the best approach.

7. Technical points

There are numerous technical controls that can be put in place to mitigate risk and help ensure compliance with PCI DSS. The following are the most important.

User access: User access to any part of your IT environment should be controlled. There should be a defined set of policies, procedures, standards and guidelines to restrict what a user can do and what resources are available to any person.

Change management: Management of change to all systems associated with payment card processing should be a defined process within your organisation. It is relatively straightforward to get compliant at

(Continued on page 13)

(Continued from page 12)

a point in time, but the goal is stay compliant consistently. A quality change management process is one of the key factors that separates high-performing IT environments from low-performing ones. Your systems must change and evolve, so make sure you are capable of managing and controlling those changes.

Implement defence in depth: At a minimum, your organisation needs to have implemented an intrusion detection system, virus control, and network segmentation to be in compliance with the PCI DSS. Simply having a firewall is not enough. You need strong perimeter controls that can deal with sophisticated threats. Malicious software of all kinds, e.g. viruses, worms, spyware and ‘zero-day’ exploits have raised the bar on protection requirements. Defence in depth is a strategy based on multiple layers of defence. In general, a security posture that does not rely on any single vendor, application, or device, is more likely to be a successful one. Internal and external vulnerability assessments and penetration tests should be conducted on at least a quarterly basis.

Harden servers: Servers that store and process credit card data or are internet facing must be configured securely and adhere to documented configuration standards. For example, all unnecessary services should be disabled, user access should be strictly controlled and logged, access permissions should restrict access to key files, and all critical files and programs should be carefully monitored for unauthorised changes. A vulnerability management program that includes implementing system patches in a timely manner also needs to be in place, but be aware applying all available patches can compromise the stability of systems and present a greater risk than that of deferring lower priority patches.

Control vendor and remote access: Access to databases and point of sale systems is typically enabled for third parties who provide support services. This type of access bypasses network firewalls and access control, and the access may not be logged. It is recommended to implement strong access controls for all users, especially ones with remote access, detailed logging, and two

factor authentication for remote access users.

Implement detailed system logging: Any part of your IT environment that processes credit cards or controls network access to important systems needs to have tamper-resistant logs enabled. In the event of a security or data breach, information from logs can be crucial when trying to determine what happened, how much information was compromised, and by whom. However, merely enabling logging can provide a false sense of security — realising the benefits of logging requires the logs to be monitored and exceptions resolved, which in turn depends on the exception criteria being set so as not to generate too many false positives.

Do not store credit card numbers: Despite the potential usefulness of credit card data for business intelligence purposes, it is forbidden to store the primary account number or any of the other elements known as track 2 on the magnetic stripe or any “card not present” data (card validation codes). After the card transaction is authorised and the payment is processed, the card number should be masked, track 2 data should be deleted, and assurance should be obtained that the data are not stored in any logs.

Design and development of applications: If you are one of the organisations that develops their applications in-house or engages a third party to develop bespoke applications, you should ensure that the systems development lifecycle has adequate controls to ensure that the security of your entire IT environment, not just the security of the credit card data, is maintained. A third-party report such as a SAS 70 could give assurance that this process is controlled.

Security policy: A security policy is a requirement of the DSS. Third-party contracts also need to include clauses stating that third parties will comply with PCI standards and, in the case of a security breach, there is a right to audit and conduct forensic analysis. A security policy is a valuable thing to have in place and, if it is properly structured and exists within the context of a suitably worded contract (e.g. an employment

contract), it is in effect an agreement between the owners of the system and the end users that all activities and interactions with systems and data are approved and authorised and follows standard processes. Good security policies will improve business practices and will facilitate a better understanding of security practices.

General awareness and formal training

It is widely acknowledged that end-users are, often unwittingly, the weakest link in a security program, and social engineering — tricking users into divulging secure information — is often the easiest way for a cyber-criminal to breach an organisation’s IT security measures. Your organisation should have senior level management support for any IT security program, and there needs to be clear demonstration of how IT security supports the organisation’s goals, and how important it is that all users actively participate. Appropriate training and communications needs to be adapted for the audience. Training that is too basic will be ignored, and if it is too technical it will not be understood. A once-off security presentation will be forgotten by many by the time they return to their desks—the key aspects of the training must be made part of the organisation’s culture.

Next steps

An article such as this can only serve as an introduction to the topic of PCI DSS compliance, but like most compliance projects, reliance on a few basic principles and a willingness to focus on risk, and re-engineer processes for cost efficiency as well as compliance effectiveness, can reduce the burden to a manageable level. Following each of the principles above will put any organisation firmly on the road to cost-effective PCI DSS compliance.

**Cian Blackwell and
Mark Gahan**

Grant Thornton

cian.blackwell@grantthornton.ie

mark.gahan@grantthornton.ie
