

# Understanding the 12 Requirements of PCI DSS

Practical steps to achieve and maintain compliance



Regardless of whether you are a retailer, service provider or a bank, if you process any form of credit or debit card data you have to ensure a thorough understanding of the Payment Card Industry Data Security Standard (PCI DSS) and how it impacts your organisation, writes Brian Pennington, Business Development Manager at Dimension Data UK.

Cardholder information is increasingly becoming a target for cyber thieves. In an attempt to secure transactions and personal data, the PCI Security Standard Council drafted the Data Security Standard (PCI DSS). This standard applies to every organisation that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit data.

The 12 requirements specified in the DSS are structured under five key areas to ensure that there are no loopholes when it comes to securing cardholder transaction and personal data.

#### The key areas are:

- Building and maintaining a secure network (**requirement 1 – 4**)
- Maintaining a vulnerability management programme (**requirements 5 – 6**)
- Implementing strong access control measures (**requirements 7 – 9**)
- Regularly monitoring and testing networks (**requirements 10 – 11**)
- Maintaining an information security policy (**requirement 12**)

Although the DSS is clearly structured, there is no doubt that organisations may find it challenging to interpret how they match their overall security roadmap and also previous investments in technology and processes. A single violation of any of the requirements can trigger an overall non-compliant status resulting in fines, suspension and revocation of card processing privileges.

## In an attempt to **secure transactions and personal data**, the PCI Security Standard Council drafted the **Data Security Standard (PCI DSS)**.

### Demystifying the DSS requirements

Understanding what the requirements of the PCI DSS mean to your organisation and being able to articulate this outside the IT department is a crucial first step in achieving and maintaining compliance.

#### **Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

**Key action:** To comply with this standard you have to demonstrate that your firewalls and routers are correctly maintained and independently tested.

#### **Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

**Key action:** A firewall is a fundamental part of network security. Following on from our first step, a correctly implemented firewall will automatically comply with this requirement, but is it really that easy? The answer is 'yes' as long as you can prove that the appropriate steps have been taken both during the implementation phase and afterwards under change management. Again, it is about process and people – not simply products that provide a technical solution. The requirement also includes Wireless LANs since the v1.2 clarification/update.

#### **Requirement 3: Protect stored cardholder data**

**Key action:** All stored data must be encrypted. If you assess where the credit card data is stored you can quickly achieve compliance using any one of several commercially available tools. Some details should never be stored, e.g. PIN numbers and the full details on the magnetic strip.

#### **Requirement 4: Encrypt transmission of cardholder data across open, public networks**

**Key action:** The highly distributed nature of today's supply chain and service relationships creates a dependency on public networks. In view of this, the easiest way to fail this requirement is by not addressing how your wireless network and remote access solutions are configured. Most other transmissions can be configured to use VPN software such as SSL & IPSec. Mapping the route of the transmission will quickly show where encryption is required. From 31st March 2009 Wireless Networks using the WEP encryption standard will no longer be allowed to transmit credit card data of any type.

#### **Requirement 5: Use and regularly update anti-virus software**

**Key action:** Cyber criminals' capabilities to break into networks are increasing at an alarming rate. Although organisations have anti-virus software to safeguard against attacks, they need to ensure that the frequently published updates reach every device.

The clarification in v1.2 of the PCI DSS standard notes that anti-malware protection is to include all operating systems and all forms of malware. Intrusion detection or prevention systems are becoming an even more important form of protection, because they do not need regular patching (unlike anti-virus software which fundamentally depends on it) and they can be both device and network aware. Install these systems in front of the devices storing credit card details to ensure maximum protection. Alternatively, to ensure that all your anti-virus software is patched, make a comparison between the total number of devices connected with the number that is being updated. In addition, Network Access Control (NAC) is a mechanism to ensure that anti-virus patches have been applied to individual workstations as they attempt to connect to the network.

### **Requirement 6: Develop and maintain secure systems and applications**

**Key action:** In an increasingly complex and integrated world of applications, middleware and servers, maintaining a comprehensive view of security is a major challenge. Review the alerts of all the software vendors used in your systems and apply their patches methodically. If the application has been customised, patching can be very difficult as the extended code may be affected by the patch. In this situation, the application needs to be properly tested to see whether the application is vulnerable and then a plan must be put in place to address any issues. In addition, organisations with customised applications may consider conducting a vulnerability assessment. Version 1.2 of the standard indicates that a risk based approach may be used to prioritise patching. In addition, 6.6 which governs web based applications and their protection is now mandatory. This means the application code needs to be either regularly assessed or protected by an “application firewall”. For some merchants both the application checking and application firewall are mandatory.

### **Requirement 7: Restrict access to cardholder data by business need-to-know**

**Key action:** Access to critical data should be restricted and recorded. For example, access should only be given to staff working with credit/debit card details. Remember, through the use of encryption and directory access controls, it is possible to allow administrators and support staff appropriate access to the services they need without them seeing sensitive data. Important to note, however, is that all access should be documented and regularly audited.

### **Requirement 8: Assign a unique ID to each person with computer access**

**Key action:** It is a well-known fact in the industry that the majority of database breaches are internal. Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorised users. All remote users should access the data via two factor authentications (e.g. tokens or smartcards). In addition, inactive devices should be logged off after a pre-determined period of inactivity. It is a requirement of this standard to have passwords tested to prove they are unreadable during transmission and storage.

### **Requirement 9: Restrict physical access to cardholder data**

**Key action:** Physical access to any building needs to be via a reception area with all visitors and contractors signing in. All devices that store or could store credit card details have to be in a secure environment. Server rooms need to be locked with CCTV installed. Access to the wireless and wired network components must be restricted.

### **Requirement 10: Track and monitor all access to network resources & cardholder data**

**Key action:** The logs of the network and appropriate devices need to be recorded and analysed for anomalies. The logs need to be stored so that legitimate access, intrusions and attempted intrusions can be tracked. The logs must be available as evidence in case of a breach and this can be achieved by using log management, Security Event Management (SEM) and Security Information and Event Management (SIEM). All external system logs e.g. wireless, firewalls, DNS etc must be stored internally. Penetration tests do not have to be undertaken by QSAs (Qualified Security Advisors) or ASVs (Approved Scan Vendors).

### **Requirement 11: Regularly test security systems and processes**

**Key action:** All organisations that are affected by the PCI DSS regulations should conduct regular vulnerability scans for possible exploitable weaknesses. When there are significant changes to the network, device operating systems or applications, organisations should run internal and external vulnerability scans.

### **Requirement 12: Maintain a policy that addresses information security**

**Key action:** Business is becoming more dependent on IT and the organisation therefore needs to be more aware of IT security as part of their overall policies and risk management strategies. Ownership of this must be assigned to a person or group within the organisation. A strong security policy sets the tone for the entire company and informs employees of what is expected of them. This standard specifies that critical employee facing technologies includes remote access technologies, wireless technologies, removable electronic media, email usage, internet usage, laptops, and Personal Data Assistants (PDAs). The standard also states that service providers should be monitored and managed.

In an **increasingly complex and integrated world of applications, middleware and servers, maintaining a comprehensive view** of security is a major challenge.

As a first step, it is **important to build a roadmap** to determine your existing status and **future goals**, because the requirements on the different merchants and provider levels will affect your approach to the project.

### Proactive steps to become compliant

Once you understand the requirements, it is recommended that you communicate these to the broader organisation and follow proactive steps to achieve and maintain PCI DSS compliance without losing sight of your overall IT security posture.

#### **Step 1: Build a roadmap**

As a first step, it is important to build a roadmap to determine your existing status and future goals, because the requirements on the different merchants and provider levels will affect your approach to the project. Each project should have an agreed start, target and end date and should be assigned the right resources within your business to ensure successful implementation. A resource within the IT department or if appropriate, the entire business, should be tasked with keeping abreast of new threats and any impending changes/additions to the PCI DSS requirements. This ensures that you can adapt your roadmap and milestone projects accordingly.

In addition, validation should be an ongoing effort with quarterly and annual tasks, including onsite assessments and audits, self-assessment questionnaires and quarterly security scanning of all Internet-accessible systems and applications.

#### **Step 2: Assess performance and risk**

Organisations need to conduct a thorough assessment of where personal account data is held. They need to understand where weaknesses exist and how they need to be addressed. Without conducting this assessment, virtually no retailer can be anything more than reactive in their data security practice.

Once the assessment is completed, you should map PCI mandatory requirements and government regulations to current business processes and systems. This is an important step since mandates and regulations may overlap, and also to ensure previous investments and work is leveraged. Once this mapping exercise has been completed, you can then prioritise changes to both operational processes and systems.

#### **Step 3: Build a secure architecture**

Once assessments have taken place organisations need to build an architecture that supports the overall IT security and compliance roadmap. This often includes re-architecting the existing network and security controls to create an architecture that can address changes in the 12 requirements.

In an ideal world, all consumer-specific data, not just payment data, should be encrypted. While the PCI DSS has very specific requirements regarding encryption of personal account numbers, forward-thinking organisations should view this as an opportunity to remain at least one step ahead of industry mandates and potential legislation.

#### **Step 4: Develop appropriate storage, retrieval and disposal processes**

The vast majority of retailers, large and small, hold on to sensitive data for a period of two years. However, many experts strongly advise, "Don't store it if you don't need it" as the golden rule of data security risk avoidance. Businesses need to become more systematic in the destruction of transactional data once the business purpose for keeping it has passed.

#### **Step 5: Proactively monitor and manage the network**

While larger organisations seem to be more focused on ensuring that sensitive data remains secure throughout the life cycle of business applications, businesses of all sizes find tracking and monitoring a major business challenge. This can be mitigated by enacting clear policies of network administration, but again, can only be accomplished once full understanding of the "real view" of current practices is attained. Logging and monitoring are key technology enablers in ensuring a secure network, as are frequent network penetration tests.

In addition, having a centralised control framework allows companies to effectively implement policies while providing a linkage to business controls, including controls over financial reporting. It helps protect sensitive information from unauthorised disclosure, safeguards the accuracy and completeness of information, ensures that information and vital IT services are available when required, and provides information and services with a high level of efficiency.

In conclusion, it is crucial that IT organisations build a platform to achieve PCI compliance and maintain the appropriate level of compliance going forward. Organisations that successfully demonstrate to executives what their current security practices are through a consolidated view, where the dangers lie, and what their practices should be as defined by industry regulations and benchmarks, have a far greater chance of defining the financial risk that surrounds non-secured customer-specific data and securing appropriate boardroom commitment and investment.

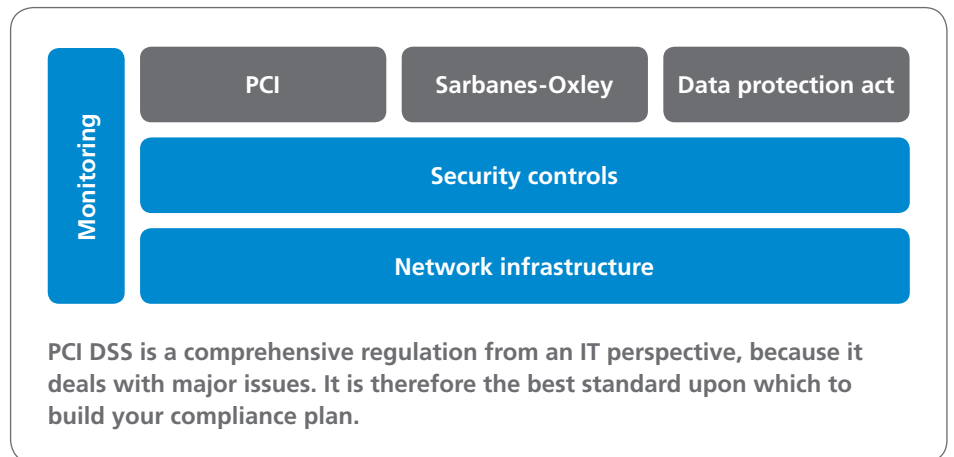
## The building blocks of compliance

Many of the controls required for the various regulatory and governance requirements are common. Understanding what regulations affect your business will enable you to map the common activities into an overall compliance plan.

## Why should PCI DSS be the basis of your compliance plan?

### It assists you to:

- Build and maintain a secure network and thereby ensuring that you have the most appropriate network technology and configurations for your business
- Maintain a vulnerability management programme which is about maintaining the network correctly and having the right malware protection for your systems
- Implement strong access control measures which entail who can access what data and how you control their access
- Regularly monitor and test networks to prove that malicious activity is not occurring
- Maintain an information security policy, which is often conducted at too high a level. The definitions in the PCI DSS standards allow for a greater level of control which in turn leads to more effective management



**MIDDLE EAST & AFRICA**

ALGERIA • ANGOLA  
BOTSWANA • GHANA • KENYA  
MOROCCO • NAMIBIA • NIGERIA  
SAUDI ARABIA • SOUTH AFRICA  
TANZANIA • UGANDA  
UNITED ARAB EMIRATES

**ASIA**

CHINA • HONG KONG  
INDIA • INDONESIA • JAPAN  
KOREA • MALAYSIA  
NEW ZEALAND • PHILIPPINES  
SINGAPORE • TAIWAN  
THAILAND • VIETNAM

**AUSTRALIA**

AUSTRALIAN CAPITAL TERRITORY  
NEW SOUTH WALES • QUEENSLAND  
SOUTH AUSTRALIA • VICTORIA  
WESTERN AUSTRALIA

**EUROPE**

BELGIUM • CZECH REPUBLIC  
FRANCE • GERMANY  
ITALY • LUXEMBOURG  
NETHERLANDS • SPAIN  
SWITZERLAND • UNITED KINGDOM

**AMERICAS**

BRAZIL • CANADA • CHILE  
MEXICO • UNITED STATES