

Contrasting Payment Card Industry Data Security Standard (PCI DSS) compliance solutions with a best practices approach to information security

By Alan Belshaw

If you are an organization that processes credit or debit card information, including merchants and third-party service providers that accept, capture, store, process or transmit credit or debit card data (both electronic and non-electronic); then compliance with PCI DSS is not a request, or a suggestion, but a requirement. A single violation of any of the requirements can trigger an overall non-compliant status. Each non-compliant incident will result in steep fines, suspension and revocation of card processing privileges.

What is PCI DSS?

PCI DSS is not about data security; it is about credit card data security. This does not mean that PCI DSS cannot provide a great framework for non-credit card data security as well. This paper is not intended to be an analysis of the PCI DSS. Rather, it is a common sense look at a range of information security wisdoms and best practices that can be used to assist in being in compliance with PCI DSS, while having the additional effect of increasing an organization's overall security posture. However, it is important to summarize PCI DSS and define credit card data security, so that a frame of reference exists to understand the usefulness of these wisdoms and best practices.

At face value, PCI DSS is a 6 goal and 12 requirement program; but these 12 requirements break into some 240 detailed line items. The current standard is 1.1, with PCI DSS 1.2 expected to be released in October 2008. No details have yet been released pertaining to the new standard, but it is rumored to be evolutionary rather than revolutionary. The 6 goals and 12 requirements are as follows:

1) 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

2) Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

3) Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

4) 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

5) 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

6) Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Compliance validation is a pass/fail grade, can vary by brand and merchant level. Compliance certification is done by the Acquirers (banks), who set the merchant levels and approve any compensating controls. The validation process involves the annual Self-Assessment Questionnaire (SAQ)¹ and a Qualified Security Assessor (QSA). There are also quarterly network scans to be done by an Approved Scanning Vendor (ASV). The network scans use a rating of 1 through 5, and everything past a 3 needs to be corrected. It is not unusual to fail the network scan on the first try. Finally, the imposition of fines and sanctions is done by the payment brands, who also define (not set) the merchant levels and enforce the standard.

Where to start?

Everything starts with the cardholder data. First thing is to realize that both electronic and non-electronic data is in scope (the highest risk area will actually be the face-to-face transactions rather than ecommerce). Secondly, if you don't need it, don't store it. If you still want to store it, the trick is to know what you can store and what you can't; as well as how you need to protect the data elements that you can store. You can store some cardholder data elements (from the front of the card) if they are protected, but you can't store sensitive authentication data (from the back of the card):

Element of Data	Is Storage Allowed?	Is Protection Required?	PCI DSS Requirement 3.4	
Primary Account Number (PAN)	YES	YES	YES	Cardholder Data (Front of Card)
Cardholder Name*	YES	YES*	NO	
Service Code*	YES	YES*	NO	
Expiration Date*	YES	YES*	NO	
Full Magnetic Strip	NO	N/A	N/A	Sensitive Authentication Data (Back of Card)
CVC2/CVV2/CID	NO	N/A	N/A	
PIN/PIN Block	NO	N/A	N/A	

* These data elements must be protected if stored in conjunction with the PAN

Although the card holder data on the front of the card can be retained (both PCI DSS and the payment card brands discourage this unless there is a business need), it must be protected. Protection of data means that it needs to be encrypted or otherwise made unreadable (PCI DSS Requirement 3.4²).

Knowing which data elements that may be kept for the charge back process is often an area that can cause confusion. Sensitive authentication data, such as CVV2, are used for charge back verification but must not be stored. The entire 16 digit Primary Account

¹ <http://www.pcisecuritystandards.org/saq/index.shtml>

² http://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

Number (PAN) cannot be kept in an unprotected mode. Only the first 6 and the last 4 digits can be stored in this manner, because in this form, they are not card holder data. So, for example³;

- **Name + Expiry Date + Service Code** is not cardholder data because the PAN is not retained
- **1234 5678 9012 3456 + Name + Expiry Date** is cardholder data because the PAN is retained; so everything must be protected
- **1234 56xx xxxx 3456 + Name + Expiry Date** is not cardholder data because store the first 6 and the last 4 digits unprotected
- **1234 56xx xxxx 3456 + Name + CVV2** cannot be stored since sensitive authentication data is retained

These rules also apply to digital voice and fax systems. Digital voice systems are searchable, so if a recording contains sensitive authentication data (CVV2/CVC2/CID), it cannot be stored and must be cleaned. It is also a good idea to restrict physical and logical access to such voice systems. Fax paper records also need to have sensitive authentication data deleted, so it is a good idea to use a form in which a section can be removed. Remember also that if your fax system has memory, that too needs to have the sensitive authentication data erased. Additionally, these rules apply to any third party providers that you use for outsourcing; so ensure that they are PCI compliant as part of your contract with them.

PCI DSS compliance equates to good security

Now that you know what to protect and why, what are some of the information security pearls of wisdom (in no particular order) that the PCI DSS industry experts are recommending that you should be doing anyway?

- 1) **Secure top management commitment⁴**: No surprise here. Any security initiative that affects the whole enterprise has to start with senior management support and be part of the security policy. To make this happen you need to put together a good business case of what needs done, why it needs done, and the cost of non-compliance if you don't do it.
- 2) **Write compliance oriented policies**: Research, compile and understand all of the compliance laws, regulations and standards that your organization is required to address. Then write policies that specifically address both organizational needs along with specific compliance requirements.
- 3) **Write policy oriented procedures**: The operational steps detailed within your procedures should ensure adherence to your policies. It is important to understand that your procedures should not only detail how tasks should be done, but also how they are actually done. Failure to deal with this will result in procedures that support your compliance oriented policies, but that do not actually get followed.

³ <http://www.walterconway.com/>

⁴ <http://www.afponline.org/>

- 4) **Leverage an established compliance framework:** Why try to reinvent the wheel? Compliance frameworks can assist organizations in documenting all of their controls and minimizing them to a list that is manageable and easy to understand. Not only can this assist in aligning controls with audit objectives, but it also allows for regular and proactive self-assessment of IT control processes that can help the organization pinpoint problems as soon as or before they arise.
- 5) **Create a verifiable change management process:** Continuous and inevitable change within the organization leads to the requirement for IT controls to evolve in response. When an organization can control and manage change on a continuous basis, it gains the visibility necessary to ensure that its infrastructures are secure, compliant and effective.
- 6) **Conduct a high level IT risk assessment:** Although this is no replacement for more detailed risk assessments of specific departments, processes or systems, a high level IT risk assessment will give you a good starting point for understanding your current security posture, use (or not) of controls, and initial gap analysis (where you are versus where you need to be).
- 7) **Facilitate training and continued education:** Increase the awareness in your user base by ensuring the right people get the right sort of training. Develop a user manual of guidelines and responsibilities. Make sure that your people keep up to date with changes in requirements via alerts, blogs and bulletins. Update your policies and procedures to facilitate this approach.
- 8) **Have a response plan:** This should exist for any type of breach that may affect your organization. It should detail how to recognize a breach, what to do (and what not to do), who to contact, and how to handle potentially compromised servers so that forensic evidence is preserved.
- 9) **Restrict your potential compliance scope:** When storing and managing any sort of private or protected information, access control is key. Use firewalls to segment your network. Control bridging between wired and wireless networks. Limit the storage of the information to well protected, hardened, well managed key servers which restrict user access on a need to know basis, utilize controls such as encryption, and have all the current anti-malware, application and operating system updates installed.
- 10) **Learn from the mistakes of others⁵:** Once you have identified the threats that your organization faces, find out not only what will be the right things to do to avoid or mitigate them, but also what things are most commonly not done and result in a breach or incident. In the case of PCI DSS non-compliance, the most frequent failures are:
 - Failure to protect stored information by allowing unencrypted data and unsecured systems (requirement #3)
 - Failure to properly test point of sale systems (POS) and web application vulnerabilities (requirement #11)
 - Failure to properly implement unique IDs due to default or weak passwords (requirement #8)

⁵ https://www.verisign.com/static/PCI_REASONS.pdf

- Failure to track access using logs and other audit monitors (requirement #10)
- Failure to segment card data using firewall technology (requirement #1)
- Failure to change insecure default passwords (requirement #2)
- Failure to maintain properly patched systems (requirement #6)

11) Maintain a systems inventory and network diagrams: Part of controlling access to systems with any sort of private or protected information is to know which other systems could potentially be used to access them. Not only will an inventory give you an insight into the state of management of all of your systems, but it should be able to assist you in identifying potential problems. For instance, some older POS terminals and software were designed to track the very data that you are trying to eliminate or restrict. For this reason, it's a good idea not to buy or sell terminals on public forums such as eBay since equipment obtained from anonymous sources may contain malicious recording and transmitting software installed by those who want the data which you process.

12) Do your own network and application scans: Regularly scan any internal and external devices that store, transmit or process any sort of private or protected information. This will help you identify potentially vulnerable application and operating system software and configurations. Be sure also to test all new software and applications for vulnerabilities that may compromise your security posture before you install them. Even better, buy applications that are PCI DSS compliant.

13) Create data flow charts⁶: When dealing with any sort of private or protected information, it is important to know where the information enters, travels through and exits a system. A data flow, such as an alignment matrix, can illustrate this to show if the design of the data flow matches what occurs in reality. Other important features of the data flow is that it can help you understand the scope of the system you have to protect, and illustrate how you can't change one component in a system without affecting all of the others.

		Providing Data				
		Card Swipe	POS Terminal	POS Terminal	Pay Flow	Bank
Receiving Data	Card Swipe					
	POS Terminal					
	POS Controller					
	Pay Flow					
	Bank					

Step #1: The Design Interface Matrix maps the data flow as it was designed to occur.

⁶ <http://issa.brighttalk.com/node/268>

		Providing Data				
		Card Swipe	POS Terminal	POS Terminal	Pay Flow	Bank
Receiving Data	Card Swipe					
	POS Terminal					
	POS Controller					
	Pay Flow					
	Bank					

Step #2: The Team Interaction Matrix maps the data flow as it actually occurs.

		Providing Data				
		Card Swipe	POS Terminal	POS Terminal	Pay Flow	Bank
Receiving Data	Card Swipe					
	POS Terminal					
	POS Controller					
	Pay Flow					
	Bank					

	No Interface
	Matched Interface
	Unidentified Interface
	Unattended Interface

Step #3: The Alignment Matrix maps the Design Interface Matrix against the Team Interaction Matrix. Unidentified interfaces will need to be located, and unattended interface be protected from exposure.

14) Consider log management software⁷: One of the ironies of good security practices is that if you are logging a sufficient amount of information, you probably will not have sufficient time to properly analyze it. It is worth investigating automated log management tools to assist in this function. Such tools can automatically collect diverse log types from distributed sources,

⁷ <http://www.gfi.com/whitepapers/automated-event-log-management-for-pci-dss.pdf>

consolidate them in a central repository, sift out trivial events, generate alerts on key events, and incorporate report management capabilities.

15) Look at different ways to use encryption⁸: When dealing with any sort of private or protected information, apart from not storing it at all, encryption is probably the next most effective control. It is also a “defense in depth” control meaning that if other protection mechanisms are bypassed and unauthorized access to information is acquired, the information will be unreadable if it is encrypted. There are also a number of options regarding implementing an encryption solution:

- *Retrofitting all applications:* Encryption is rolled into the coding of an application, so information entered into that application is encrypted on input.
- *Using an encryption appliance:* The appliance sits between an input application and the database, encrypting information sent to the database, and decrypting information retrieved from the database.
- *Using an encrypting database:* Encryption is done on the database, so organizations do not need to modify their existing input applications, or buy new ones.
- *Obfuscating without encryption:* This is using approaches such as one-way hashing and truncation to make information unreadable, rather than implementing a more costly encryption solution.

16) Utilize intrusion detection/prevention technology: Intrusion Detection/Protection Systems can give you a unique insight to the network based on both known attack signatures, and data anomalies and variations from your baseline. A word of caution about using the latter; it may take several weeks to months to build up an anomalies and variations database that has enough “intelligence” such it is useful in identifying exceptions and avoiding false positives. Additionally, these devices operate at the network layer, and other solutions (such as application log monitoring) will be needed to identify potential threats at the application layer.

17) Utilize automation in testing IT controls: The more the human element can be eliminated from the process of testing, the greater the level of preparedness, consistency and accuracy that can be achieved. Additionally, IT staff efforts can be redirected towards other key issues that the organization needs addressed.

Finally, remember the easiest way to comply with PCI DSS is not to keep cardholder data. If you do need to keep it, bear in mind the five stages of PCI Grief:

1. **Denial** (it doesn't apply to me): PCI DSS compliance is mandatory
2. **Anger** (it isn't fair): PCI DSS compliance applies to everybody
3. **Bargaining** (we will do some of it): PCI DSS compliance is pass/fail
4. **Depression** (we will never get there): many merchants already have
5. **Acceptance** (adoption of industry best standards): PCI DSS compliance addresses things you should be doing already anyway.

⁸ <http://www.securepayments.com/resources/verisign-pci-audit-tips.pdf>