The Prioritized Approach to Pursue PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) provides a detailed, 12 requirements structure for securing cardholder data that is stored, processed and/or transmitted by merchants and other organizations. By its comprehensive nature, the standard provides a large amount of information about security – so much that some people who are responsible for cardholder data security may wonder where to start the continuous journey of compliance. Toward this end, the PCI Security Standards Council provides the following Prioritized Approach to help stakeholders understand where they can act to reduce risk earlier in the compliance process. No single milestone in the Prioritized Approach will provide comprehensive security or PCI DSS compliance, but following its guidelines will help stakeholders to expedite the process of securing cardholder data.

HIGHLIGHTS

Can help merchants identify highest risk targets

Creates a common language around PCI DSS implementation and assessment efforts

Milestones enable merchants to demonstrate progress on compliance process

What Is the Prioritized Approach?

The Prioritized Approach provides six security milestones that will help merchants and other organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance. The Prioritized Approach and its milestones (described on page 2) are intended to provide the following benefits:

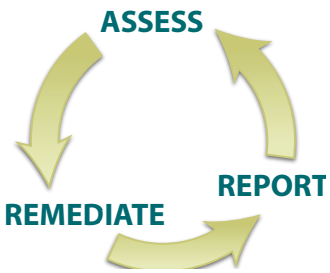
- Roadmap that an organization can use to address its risks in priority order
- Pragmatic approach that allows for “quick wins”
- Supports financial and operational planning
- Promotes objective and measurable progress indicators
- Helps promote consistency among assessors

Objectives of the Prioritized Approach

The Prioritized Approach provides a roadmap of compliance activities based on risk associated with storing, processing, and/or transmitting cardholder data. The roadmap helps to prioritize efforts to achieve compliance, establish milestones, lower the risk of cardholder data breaches sooner in the compliance process, and helps acquirers objectively measure compliance activities and risk reduction by merchants, service providers, and others. The Prioritized Approach was devised after factoring data from actual breaches, and feedback from Qualified Security Assessors, forensic investigators, and the PCI Security Standards Council Board of Advisors. It is not intended as a substitute, short cut or stop-gap approach to PCI DSS compliance, nor is it a mandatory one-size-fits-all framework applicable to every organization. The Prioritized Approach is suitable for merchants who undergo an on-site assessment or use SAQ D.

May 2011

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



PCI SSC FOUNDERS

American Express
Discover
JCB
MasterCard Worldwide
VISA

PARTICIPATING ORGANIZATIONS

Merchants, banks, processors, developers and point of sale vendors

Disclaimer

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. This document does not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice. PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation whatsoever regarding the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.

Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The matrix below summarizes the high-level goals and intentions of each milestone. The rest of this document maps the milestones to each of all twelve PCI DSS requirements and their sub-requirements.

Milestone	Goals
1	**Remove sensitive authentication data and limit data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	**Protect the perimeter, internal, and wireless networks.** This milestone targets controls for points of access to most compromises – the network or a wireless access point.
3	**Secure payment card applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	**Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	**Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protections mechanisms for that stored data.
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

May 2011

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
Requirement 1: Install and maintain a firewall configuration to protect cardholder data								
1.1	Establish firewall and router configuration standards that include the following:							6
	1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations						
	1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks	1					
	1.1.3	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone		2				
	1.1.4	Description of groups, roles, and responsibilities for logical management of network components						6
	1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure		2				
	1.1.6	Requirement to review firewall and router rule sets at least every six months						6
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.			2				
	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.		2				
	1.2.2	Secure and synchronize router configuration files.		2				
	1.2.3	Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.		2				
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.			2				
	1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		2				
	1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.		2				
	1.3.3	Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.		2				
	1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.		2				
	1.3.5	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.		2				

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
	1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)		2				
	1.3.7	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.		2				
	1.3.8	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: • Network Address Translation (NAT) • Placing servers containing cardholder data behind proxy servers/ firewalls or content caches, • Removal or filtering of route advertisements for private networks that employ registered addressing, • Internal use of RFC1918 address space instead of registered addresses.		2				
1.4		Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.		2				
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters								
2.1		Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.		2				
	2.1.1	**For wireless environments** connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.		2				
2.2		Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.			3			
	2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*			3			

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
	2.2.2	Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.			3			
	2.2.3	Configure system security parameters to prevent misuse			3			
	2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.			3			
2.3		Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for Web-based management and other non-console administrative access.		2				
2.4		Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers*.			3			
Requirement 3: Protect stored cardholder data								
3.1		Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes as follows:	1					
	3.1.1	Implement a data retention and disposal policy that includes: Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. • Processes for secure deletion of data when no longer needed. • Specific retention requirements for cardholder data. • A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	1					
3.2		Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3. *Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.*	1					
	3.2.1	Do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	1					
	3.2.2	Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions	1					
	3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	1					

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).					5	
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.*					5	
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.					5	
3.5	Protect any keys used to secure cardholder data against both disclosure and misuse *Note: This requirement also applies to key encryption keys used to protect data encrypting keys – such key encryption keys must be at least as strong as the data encrypting key.*					5	
3.5.1	Restrict access to cryptographic keys to the fewest number of custodians necessary					5	
3.5.2	Store cryptographic keys securely in the fewest possible locations and forms					5	
3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:					5	
3.6.1	Generation of strong cryptographic keys					5	
3.6.2	Secure cryptographic key distribution					5	
3.6.3	Secure cryptographic key storage					5	

	PCI DSS Requirements	Milestone					
		1	2	3	4	5	6
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).					5	
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. *Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*					5	
3.6.6	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). *Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*					5	
3.6.7	Prevention of unauthorized substitution of cryptographic keys					5	
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities					5	
Requirement 4: Encrypt transmission of cardholder data across open, public networks							
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.		2				
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. *Note: The use of WEP as a security control was prohibited as of 30 June, 2010.*		2				
4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).		2				

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
Requirement 5: Use and regularly update anti-virus software or programs							
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).		2				
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.		2				
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.		2				
Requirement 6: Develop and maintain secure systems and applications							
6.1	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.			3			
6.2	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. *Note: Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.* *Note: The ranking of vulnerabilities as defined in 6.2.a is considered a best practice until June 30, 2012, after which it becomes a requirement.*			3			
6.3	Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:			3			
6.3.1	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.			3			
6.3.2	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development lifecycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*			3			
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:			3			
6.4.1	Separate development/test and production environments			3			

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
	6.4.2	Separation of duties between development/test and production environments			3			
	6.4.3	Production data (live PANs) are not used for testing or development			3			
	6.4.4	Removal of test data and accounts before production systems become active			3			
	6.4.5	Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:						6
		6.4.5.1 Documentation of impact.						6
		6.4.5.2 Documented change approval by authorized parties.						6
		6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.						6
		6.4.5.4 Back-out procedures.						6
6.5	Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: *Note: The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*				3			
	6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XpPath injection flaws as well as other injection flaws.			3			
	6.5.2	Buffer overflow.			3			
	6.5.3	Insecure cryptographic storage.			3			
	6.5.4	Insecure communications.			3			
	6.5.5	Improper error handling.			3			
	6.5.6	All “High” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2). *Note: This requirement is considered a best practice until June 30, 2012, after which it becomes a requirement.*			3			
	Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external):							
	6.5.7	Cross-site scripting (XSS).			3			
	6.5.8	Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).			3			
	6.5.9	Cross-site request forgery (CRSF).			3			

May 2011

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing a web-application firewall in front of public-facing web applications			3			
Requirement 7: Restrict access to cardholder data by business need to know							
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:				4		
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities				4		
7.1.2	Assignment of privileges is based on individual personnel's job classification and function				4		
7.1.3	Requirement for a documented approval by authorized parties specifying required privileges				4		
7.1.4	Implementation of an automated access control system				4		
7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:				4		
7.2.1	Coverage of all system components				4		
7.2.2	Assignment of privileges to individuals based on job classification and function				4		
7.2.3	Default "deny-all" setting				4		
Requirement 8: Assign a unique ID to each person with computer access							
8.1	Assign all users a unique username before allowing them to access system components or cardholder data.				4		
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric				4		

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
8.3		Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) *Note: Two-factor authentication requires that two of the three authentication methods (see Req. 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.*				4		
8.4		Render all passwords unreadable during transmission and storage on all system components using strong cryptography.				4		
8.5		Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:				4		
	8.5.1	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects				4		
	8.5.2	Verify user identity before performing password resets.				4		
	8.5.3	Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.				4		
	8.5.4	Immediately revoke access for any terminated users.				4		
	8.5.5	Remove/disable inactive user accounts at least every 90 days.				4		
	8.5.6	Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.				4		
	8.5.7	Communicate authentication procedures and policies to all users who have access to cardholder data.				4		
	8.5.8	Do not use group, shared, or generic accounts and passwords, or other authentication methods..				4		
	8.5.9	Change user passwords at least every 90 days.				4		
	8.5.10	Require a minimum password length of at least seven characters.				4		
	8.5.11	Use passwords containing both numeric and alphabetic characters.				4		
	8.5.12	Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.				4		
	8.5.13	Limit repeated access attempts by locking out the user ID after not more than six attempts.				4		
	8.5.14	Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.				4		

PCI DSS Requirements			Milestone					
			1	2	3	4	5	6
	8.5.15	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.				4		
	8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.				4		
Requirement 9: Restrict physical access to cardholder data								
9.1		Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.		2				
	9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.		2				
	9.1.2	Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is specifically authorized.		2				
	9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines.		2				
9.2		Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. *Note: For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.*					5	
9.3		Make sure all visitors are handled as follows:					5	
	9.3.1	Authorized before entering areas where cardholder data is processed or maintained					5	
	9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel					5	
	9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration					5	
9.4		Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.					5	

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
9.5	Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.					5	
9.6	Physically secure all media. *Note: For the purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.*					5	
9.7	Maintain strict control over the internal or external distribution of any kind of media, including the following:					5	
9.7.1	Classify the media so the sensitivity of the data can be determined.					5	
9.7.2	Send the media by secured courier or other delivery method that can be accurately tracked.					5	
9.8	Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).					5	
9.9	Maintain strict control over the storage and accessibility of media.					5	
9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.					5	
9.10	Destroy media when it is no longer needed for business or legal reasons as follows:	1					
9.10.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	1					
9.10.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	1					
Requirement 10: Track and monitor all access to network resources and cardholder data							
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.				4		
10.2	Implement automated audit trails for all system components to reconstruct the following events:				4		
10.2.1	All individual accesses to cardholder data				4		
10.2.2	All actions taken by any individual with root or administrative privileges				4		
10.2.3	Access to all audit trails				4		
10.2.4	Invalid logical access attempts				4		
10.2 5	Use of identification and authentication mechanisms				4		
10.2.6	Initialization of the audit logs				4		
10.2.7	Creation and deletion of system-level objects				4		

May 2011

PCI DSS Requirements	Milestone					
	1	2	3	4	5	6
10.3 Record at least the following audit trail entries for all system components for each event:				4		
10.3.1 User identification				4		
10.3.2 Type of event				4		
10.3.3 Date and time				4		
10.3.4 Success or failure indication				4		
10.3.5 Origination of event				4		
10.3.6 Identity or name of affected data, system component, or resource				4		
10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.				4		
10.4.1 Critical systems have the correct and consistent time.				4		
10.4.2 Time data is protected.				4		
10.4.3 Time settings are received from industry-accepted time sources.				4		
10.5 Secure audit trails so they cannot be altered				4		
10.5.1 Limit viewing of audit trails to those with a job-related need.				4		
10.5.2 Protect audit trail files from unauthorized modifications.				4		
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.				4		
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.				4		
10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).				4		
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).				4		
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).				4		

PCI DSS Requirements	Milestone					
	1	2	3	4	5	6
Requirement 11: Regularly test security systems and processes						
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. *Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.*				4		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).		2				
11.2.1 Perform quarterly internal vulnerability scans.		2				
11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).		2				
11.2.3 Perform internal and external scans after any significant change.		2				
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:		2				
11.3.1 Network-layer penetration tests		2				
11.3.2 Application-layer penetration tests		2				
11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. *Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date.*		2				
11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.				4		
Requirement 12: Maintain a policy that addresses information security for all personnel						
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:						6
12.1.1 Addresses all PCI DSS requirements	1	2	3	4	5	6
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment	1					

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
12.1.3	Includes a review at least annually and updates when the environment changes						6
12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).						6
12.3	Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email usage and internet usage) to define proper use of these technologies. Ensure these usage policies require the following:						6
12.3.1	Explicit approval by authorized parties						6
12.3.2	Authentication for use of the technology						6
12.3.3	A list of all such devices and personnel with access						6
12.3.4	Labeling of devices to determine owner, contact information, and purpose						6
12.3.5	Acceptable uses of the technology						6
12.3.6	Acceptable network locations for the technologies						6
12.3.7	List of company-approved products						6
12.3.8	Automatic disconnect of sessions for remote access technologies after a specific period of inactivity						6
12.3.9	Activation of remote access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use						6
12.3.10	For personnel accessing cardholder data via remote access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless specifically authorized for a defined business need.						6
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.						6
12.5	Assign to an individual or team the following information security management responsibilities. Responsibility for information security formally assigned to a Chief Security Officer or other security-knowledgeable member of management.						6
12.5.1	Establish, document, and distribute security policies and procedures.						6
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.						6
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.				4		

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
12.5.4	Administer user accounts, including additions, deletions, and modifications						6
12.5.5	Monitor and control all access to data.						6
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.						6
12.6.1	Educate personnel upon hire at least annually. *Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*						
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.						6
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) *Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*						6
12.8	If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:		2				
12.8.1	Maintain a list of service providers.		2				
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.		2				
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.		2				
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.		2				
12.9	Implement an incident response plan. Be prepared to respond immediately to a system breach.				4		

PCI DSS Requirements		Milestone					
		1	2	3	4	5	6
12.9.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands				4		
12.9.2	Test the plan at least annually.				4		
12.9.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.				4		
12.9.4	Provide appropriate training to staff with security breach response responsibilities.				4		
12.9.5	Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.				4		
12.9.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.				4		
Requirement A.1: Shared hosting providers must protect the cardholder data environment							
A.1	Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4. A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.			3			
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.			3			
A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.			3			
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.			3			
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.			3			