Payment Card Industry (PCI) Data Security Standard

Security Audit Procedures

Version 1.1

Release: September 2006

Table of Contents

Introduction

The PCI Security Audit Procedures are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS.

This document contains the following:

- **Introduction**
- **PCI DSS Applicability Information**
- **Scope of Assessment for Compliance with PCI DSS Requirements**
- **Instructions and Content for *Report On Compliance***
- **Revalidation of Open Items**
- **Security Audit Procedures**

APPENDICES

- **Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)**
- **Appendix B: Compensating Controls**
- **Appendix C: Compensating Controls Worksheet/Completed Example**

PCI DSS Applicability Information

The following table illustrates commonly used elements of cardholder and sensitive authentication data; whether **storage** of each data element is permitted or prohibited; **and if each data element** must be **protected**. This table is not exhaustive, but is presented to illustrate the different types of requirements that apply to each data element.

	Data Element	Storage Permitted	Protection Required	PCI DSS REQ. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	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. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

Scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all "system components." A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

A service provider or merchant may use a third party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant services of the third party provider must be scrutinized either in 1) each of the third party provider's clients' PCI audits; or 2) the third party provider's own PCI audit.

For service providers required to undergo an annual onsite review, compliance validation must be performed on all system components where cardholder data is stored, processed, or transmitted, unless otherwise specified.

For merchants required to undergo an annual onsite review, the scope of compliance validation is focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, third party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or for devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by Internet, wireless, virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded

Wireless

If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, "line-busting"), or if a wireless local area network (LAN) is connected to or part of the cardholder environment (for example, not clearly separated by a firewall), the Requirements and Testing Procedures for wireless environments apply and must be performed as well. Wireless security is not mature yet, but these requirements specify that basic wireless security features be implemented to provide minimal protection. Since wireless technologies cannot yet be secured well, before wireless technology is put in place, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission or waiting to deploy more secure technology.

Outsourcing

For those entities that outsource storage, processing, or transmission of cardholder data to third party service providers, the *Report on Compliance* must document the role of each service provider. Additionally, the service providers are responsible for validating their own compliance with the PCI DSS requirements, independent of their customers' audits. Additionally, merchants and service providers must contractually require all associated third parties with access to cardholder data to adhere to the PCI DSS. *Refer to Requirement 12.8 in this document for details.*

Sampling

The assessor may select a representative sample of system components to test. The sample must be a representative selection of all of the types of system components, and include a variety of operating systems, functions, and applications that are applicable to the area being reviewed. For example, the reviewer could choose Sun servers running Apache WWW, NT servers running Oracle, mainframe systems running legacy card processing applications, data transfer servers running HP-UX, and Linux Servers running MYSQL. If all applications run from a single OS (for example, NT, Sun), then the sample should still include a variety of applications (for example, database servers, web servers, data transfer servers).

When selecting samples of merchants' stores or for franchised merchants, assessors should consider the following:

- If there are standard, required PCI DSS processes in place that each store must follow, the sample can be smaller than is necessary if there are no standard processes, to provide reasonable assurance that each store is configured per the standard process.
- If there is more than one type of standard process in place (for example, for different types of stores), then the sample must be large enough to include stores secured with each type of process.
- If there are no standard PCI DSS processes in place and each store is responsible for their processes, then sample size must be larger to be assured that each store understands and implements PCI DSS requirements appropriately.

Compensating Controls

Compensating controls must be documented by the assessor and included with the Report on Compliance submission, as shown in Appendix C – Compensating Controls Worksheet / Completed Example.

See PCI DSS Glossary, Abbreviation, and Acronyms for the definitions of “compensating controls.”

Instructions and Content for Report on Compliance

This document is to be used by assessors as the template for creating the *Report on Compliance*. The audited entity should follow each payment card company’s respective reporting requirements to ensure each payment card company acknowledges the entity’s compliance status. Contact each payment card company to determine each company’s reporting requirements and instructions. All assessors must follow the instructions for report content and format when completing a *Report on Compliance*:

1. Contact Information and Report Date

- Include contact information for merchant or service provider and assessor
- Date of report

2. Executive Summary

Include the following:

- Business description
- List service providers and other entities with which the company shares cardholder data
- List processor relationships
- Describe whether entity is directly connected to payment card company
- For merchants, POS products used
- Any wholly-owned entities that require compliance with the PCI DSS
- Any international entities that require compliance with the PCI DSS
- Any wireless LANs and/or wireless POS terminals connected to the cardholder environment

3. Description of Scope of Work and Approach Taken

- Version of the Security Audit Procedures document used to conduct the assessment
- Timeframe of assessment
- Environment on which assessment focused (for example, client’s Internet access points, internal corporate network, processing points for the payment card company)
- Any areas excluded from the review
- Brief description or high-level drawing of network topology and controls
- List of individuals interviewed
- List of documentation reviewed

- List of hardware and critical (for example, database or encryption) software in use
- For Managed Service Provider (MSP) reviews, clearly delineate which requirements in this document apply to the MSP (and are included in the review), and which are not included in the review and are the responsibility of the MSP's customers to include in their reviews. Include information about which of the MSP's IP addresses are scanned as part of the MSP's quarterly vulnerability scans, and which IP addresses are the responsibility of the MSP's customers to include in their own quarterly scans

4. Quarterly Scan Results

- Summarize the four most recent quarterly scan results in comments at Requirement 11.2
- Scan must cover all externally accessible (Internet-facing) IP addresses in existence at the entity

5. Findings and Observations

- All assessors must use the following template to provide detailed report descriptions and findings on each requirement and sub-requirement
- Where applicable, document any compensating controls considered to conclude that a control is in place
- *See* PCI DSS Glossary, Abbreviation, and Acronyms *for the definitions of "compensating controls."*

Revalidation of Open Items

A "controls in place" report is required to verify compliance. If the initial report by the auditor/assessor contains "open items," the merchant/service provider must address these items before validation is completed. The assessor/auditor will then reassess to validate that the remediation occurred and that all requirements are satisfied. After revalidation, the assessor will issue a new *Report on Compliance*, verifying that the system is fully compliant and submit it consistent with instructions (See above.).

Build and Maintain a Secure Network

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

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1 Establish firewall configuration standards that include the following:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	**1.1.1** Verify that firewall configuration standards include a formal process for all firewall changes, including testing and management approval of all changes to external connections and firewall configuration			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			
	1.1.2.b. Verify that the diagram is kept current			
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**1.1.3** Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the Intranet. Verify that the current network diagram is consistent with the firewall configuration standards.			
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	**1.1.4** Verify that firewall configuration standards include a description of groups, roles, and responsibilities for logical management of network components			
1.1.5 Documented list of services and ports necessary for business	**1.1.5** Verify that firewall configuration standards include a documented list of services/ports necessary for business			
1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)	**1.1.6** Verify that firewall configuration standards include justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN			
1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented	**1.1.7.a** Verify that firewall configuration standards include justification and documentation for any risky protocols allowed (for example, FTP), which includes reason for use of protocol, and security features implemented			
	1.1.7.b Examine documentation and settings for each service in use to obtain evidence that the service is necessary and secured			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
1.1.8 Quarterly review of firewall and router rule sets	**1.1.8.a** Verify that firewall configuration standards require quarterly review of firewall and router rule sets			
	1.1.8.b Verify that the rule sets are reviewed each quarter			
1.1.9 Configuration standards for routers	**1.1.9** Verify that firewall configuration standards exist for both firewalls and routers			
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.	**1.2** Select a sample of firewalls/routers 1) between the Internet and the DMZ and 2) between the DMZ and the internal network. The sample should include the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment. Examine firewall and router configurations to verify that inbound and outbound traffic is limited to only protocols that are necessary for the cardholder data environment			
1.3 Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include:	**1.3** Examine firewall/router configurations to verify that connections are restricted between publicly accessible servers and components storing cardholder data, as follows:			
1.3.1 Restricting inbound Internet traffic to internet protocol (IP) addresses within the DMZ (ingress filters)	**1.3.1** Verify that inbound Internet traffic is limited to IP addresses within the DMZ			
1.3.2 Not allowing internal addresses to pass from the Internet into the DMZ	**1.3.2** Verify that internal addresses cannot pass from the Internet into the DMZ			
1.3.3 Implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network)	**1.3.3** Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run NMAP on all TCP ports with "syn reset" or "syn ack" bits set – a response means packets are allowed through even if they are not part of a previously established session)]			
1.3.4 Placing the database in an	**1.3.4** Verify that the database is on an internal network			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
internal network zone, segregated from the DMZ	zone, segregated from the DMZ			
1.3.5 Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment	**1.3.5** Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder environment, and that the restrictions are documented			
1.3.6 Securing and synchronizing router configuration files. For example, running configuration files (for normal functioning of the routers), and start-up configuration files (when machines are re-booted) should have the same secure configuration	**1.3.6** Verify that router configuration files are secure and synchronized [for example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), have the same, secure configurations]			
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	**1.3.7** Verify that all other inbound and outbound traffic not covered in 1.2 and 1.3 above is specifically denied			
1.3.8 Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)	**1.3.8** Verify that there are perimeter firewalls installed between any wireless networks and systems that store cardholder data, and that these firewalls deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into systems storing cardholder data			
1.3.9 Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	**1.3.9** Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization's network, have personal firewall software installed and active, which is configured by the organization to specific standards and not alterable by the employee			
1.4 Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).	**1.4** To determine that direct access between external public networks and system components storing cardholder data are prohibited, perform the following, *specifically* for the firewall/router configuration implemented between the DMZ and the internal network:			
1.4.1 Implement a DMZ to filter and screen all traffic and to prohibit direct	**1.4.1** Examine firewall/router configurations and verify there is no direct route inbound or outbound for Internet			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
routes for inbound and outbound Internet traffic	traffic			
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	**1.4.2** Examine firewall/router configurations and verify that internal outbound traffic from cardholder applications can only access IP addresses within the DMZ			
1.5 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).	**1.5** For the sample of firewall/router components above, verify that NAT or other technology using RFC 1918 address space is used to restrict broadcast of IP addresses from the internal network to the Internet (IP masquerading)			

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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
2.1 Always change vendor-supplied defaults **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	**2.1** Choose a sample of system components, critical servers, and wireless access points, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)			
2.1.1 For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community	**2.1.1** Verify the following regarding vendor default settings for wireless environments: • WEP keys were changed from default at installation, and are changed anytime any one with knowledge of the keys leaves the company or changes positions			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.	• Default SSID was changed • Broadcast of the SSID was disabled • Default SNMP community strings on access points were changed • Default passwords on access points were changed • WPA or WPA2 technology is enabled if the wireless system is WPA-capable • Other security-related wireless vendor defaults, if applicable			
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 as defined, for example, by SysAdmin Audit Network Security Network (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).	**2.2.a** Examine the organization's system configuration standards for network components, critical servers, and wireless access points, and verify the system configuration standards are consistent with industry-accepted hardening standards as defined, for example, by SANS, NIST, and CIS			
	2.2.b Verify that system configuration standards include each item below (at 2.2.1 – 2.2.4)			
	2.2.c Verify that system configuration standards are applied when new systems are configured			
2.2.1 Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers)	**2.2.1** For a sample of system components, critical servers, and wireless access points, verify that only one primary function is implemented per server			
2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)	**2.2.2** For a sample of system components, critical servers, and wireless access points, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service (for example, FTP is not used, or is encrypted via SSH or other technology)			
2.2.3 Configure system security parameters to prevent misuse	**2.2.3.a** Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for their operating systems, database servers, Web servers, and wireless systems			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	2.2.3.b Verify that common security parameter settings are included in the system configuration standards			
	2.2.3.c For a sample of system components, critical servers, and wireless access points, verify that common security parameters are set appropriately			
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	**2.2.4** For a sample of system components, critical servers, and wireless access points,, verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented, support secure configuration, and that only documented functionality is present on the sampled machines			
2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.	**2.3** For a sample of system components, critical servers, and wireless access points,, verify that non-console administrative access is encrypted by: • Observing an administrator log on to each system to verify that SSH (or other encryption method) is invoked before the administrator's password is requested • Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally • Verifying that administrator access to the wireless management interface is encrypted with SSL/TLS. Alternatively, verify that administrators cannot connect remotely to the wireless management interface (all management of wireless environments is only from the console)			
2.4 Hosting providers must protect each entity's hosted environment and data. These providers must meet specific requirements as detailed in Appendix A: "PCI DSS Applicability for Hosting Providers."	**2.4** Perform testing procedures **A.1.1** through **A.1.4** detailed in Appendix A, "PCI DSS Applicability for Hosting Providers (with Testing Procedures)" for PCI audits of **Shared Hosting Providers**, to verify that **Shared Hosting Providers** protect their entities' (merchants and service providers) hosted environment and data.			

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	**3.1** Obtain and examine the company policies and procedures for data retention and disposal, and perform the following • Verify that policies and procedures include legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons) • Verify that policies and procedures include provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data • Verify that policies and procedures include coverage for all storage of cardholder data, including database servers, mainframes, transfer directories, and bulk data copy directories used to transfer data between servers, and directories used to normalize data between server transfers • Verify that policies and procedures include A programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or, alternatively, requirements for an audit, conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed business retention requirements			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.2 Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3*:*	**3.2** If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable For each item of sensitive authentication data below, perform the following steps:			
3.2.1 Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data *In the normal course of business, the following data elements from the magnetic stripe may need to be retained: the accountholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements needed for business. NEVER store the card verification code or value or PIN verification value data elements.* *Note: See "Glossary" for additional information.*	**3.2.1** For a sample of system components, critical servers, and wireless access points, examine the following and verify that the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents			
3.2.2 Do not store the card-validation value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions *Note: See "Glossary" for additional information.*	**3.2.2** For a sample of system components, critical servers, and wireless access points, examine the following and verify that the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	• Several database schemas • Database contents			
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	**3.2.3** For a sample of system components, critical servers, and wireless access points, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstance: • Incoming transaction data • Transaction logs • History files • Trace files • Debugging logs • Several database schemas • Database contents			
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).*	**3.3** Obtain and examine written policies and examine online displays of credit card data to verify that credit card numbers are masked when displaying cardholder data, except for those with a specific need to see full credit card numbers			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: • Strong one-way hash functions (hashed indexes) • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures The MINIMUM account information that must be rendered unreadable is the PAN. *If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: "Compensating Controls."*	**3.4.a** Obtain and examine documentation about the system used to protect stored data, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that data is rendered unreadable using one of the following methods: • One-way hashes (hashed indexes) such as SHA-1 • Truncation or masking • Index tokens and PADs, with the PADs being securely stored • Strong cryptography, such as Triple-DES 128-bit or AES 256-bit, with associated key management processes and procedures			
	3.4.b Examine several tables from a sample of database servers to verify the data is rendered unreadable (that is, not stored in plain text)			
	3.4.c Examine a sample of removable media (for example, backup tapes) to confirm that cardholder data is rendered unreadable			
	3.4.d Examine a sample of audit logs to confirm that cardholder data is sanitized or removed from the logs			
	3.4.e Verify that cardholder data received from wireless networks is rendered unreadable wherever stored			
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 system or Active Directory accounts). Decryption keys must	**3.4.1.a** If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local or Active Directory accounts)			
	3.4.1.b Verify that decryption keys are not stored on the local system (for example, store keys on floppy disk, CD-ROM, etc. that can be secured and retrieved only when needed)			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
not be tied to user accounts.	**3.4.1.c** Verify that cardholder data on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media)			
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse:	**3.5** Verify processes to protect encryption keys used for encryption of cardholder data against disclosure and misuse by performing the following:			
3.5.1 Restrict access to keys to the fewest number of custodians necessary	**3.5.1** Examine user access lists to verify that access to cryptographic keys is restricted to very few custodians			
3.5.2 Store keys securely in the fewest possible locations and forms	**3.5.2** Examine system configuration files to verify that cryptographic keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys			
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:	**3.6.a** Verify the existence of key management procedures for keys used for encryption of cardholder data			
	3.6.b **For Service Providers** only: If the Service Provider shares keys with their customers for transmission of cardholder data, verify that the Service Provider provides documentation to customers that includes guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and service provider)			
	3.6.c Examine the key management procedures and perform the following:			
3.6.1 Generation of strong keys	**3.6.1** Verify that key management procedures require the generation of strong keys			
3.6.2 Secure key distribution	**3.6.2** Verify that key management procedures require secure key distribution			
3.6.3 Secure key storage	**3.6.3** Verify that key management procedures require secure key storage			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
3.6.4 Periodic key changes • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually	**3.6.4** Verify that key management procedures require periodic key changes. Verify that key change procedures are carried out at least annually			
3.6.5 Destruction of old keys.	**3.6.5** Verify that key management procedures require the destruction of old keys			
3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key	**3.6.6** Verify that key management procedures require split knowledge and dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key)			
3.6.7 Prevention of unauthorized substitution of keys	**3.6.7** Verify that key management procedures require the prevention of unauthorized substitution of keys			
3.6.8 Replacement of known or suspected compromised keys	**3.6.8** Verify that key management procedures require the replacement of known or suspected compromised keys			
3.6.9 Revocation of old or invalid keys	**3.6.9** Verify that key management procedures require the revocation of old or invalid keys (mainly for RSA keys)			
3.6.10 Requirement for key custodians to sign a form stating that they understand and accept their key-custodian responsibilities	**3.6.10** Verify that key management procedures require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities			

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

Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks. *Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS).*	**4.1.a** Verify the use of encryption (for example, SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks • Verify that strong encryption is used during data transmission • For SSL implementations, verify that HTTPS appears as a part of the browser Universal Record Locator (URL), and that no cardholder data is required when HTTPS does not appear in the URL • Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit • Verify that only trusted SSL/TLS keys/certificates are accepted • Verify that the proper encryption strength is implemented for the encryption methodology in use (Check vendor recommendations/best practices)			
4.1.1 For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.	**4.1.1.a** For wireless networks transmitting cardholder data or connected to cardholder environments, verify that appropriate encryption methodologies are used for any wireless transmissions, such as: Wi-Fi Protected Access (WPA or WPA2), IPSEC VPN, or SSL/TLS			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
If WEP is used, do the following: • Use with a minimum 104-bit encryption key and 24 bit-initialization value • Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS • Rotate shared WEP keys quarterly (or automatically if the technology permits) • Rotate shared WEP keys whenever there are changes in personnel with access to keys • Restrict access based on media access code (MAC) address	**4.1.1.b** If WEP is used, verify • it is used with a minimum 104-bit encryption key and 24 bit-initialization value • it is used only in conjunction with Wi-Fi Protected Access (WPA or WPA2) technology, VPN, or SSL/TLS • shared WEP keys are rotated at least quarterly (or automatically if the technology is capable) • shared WEP keys are rotated whenever there are changes in personnel with access to keys • access is restricted based on MAC address			
4.2 Never send unencrypted PANs by e-mail.	**4.2.a** Verify that an email encryption solution is used whenever cardholder data is sent via email			
	4.2.b Verify the existence of a policy stating that unencrypted PAN is not to be sent via email			
	4.2.c Interview 3-5 employees to verify that email encryption software is required for emails containing PANs			

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
5.1 Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) *Note: Systems commonly affected by viruses typically do not include UNIX-based operating systems or mainframes.*	**5.1** For a sample of system components, critical servers, and wireless access points, verify that anti-virus software is installed			
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware.	**5.1.1** For a sample of system components, critical servers, and wireless access points, verify that anti-virus programs detect, remove, and protect against other malicious software, including spyware and adware			
5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	**5.2** Verify that anti-virus software is current, actively running, and capable of generating logs • Obtain and examine the policy and verify that is contains requirements for updating anti-virus software and definitions • Verify that the master installation of the software is enabled for automatic updates and periodic scans, and that a sample of system components, critical servers, and wireless access points servers have these features enabled • Verify that log generation is enabled and that logs are retained in accordance with company retention policy			

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	**6.1.a** For a sample of system components, critical servers, and wireless access points and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed			
	6.1.b Examine policies related to security patch installation to verify they require installation of all relevant new security patches within 30 days			
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	**6.2.a** Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities			
	6.2.b Verify that processes to identify new security vulnerabilities include use of outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2 as new vulnerability issues are found			
6.3 Develop software applications based on industry best practices and incorporate information security throughout the software development life cycle.	**6.3** Obtain and examine written software development processes to verify that they are based on industry standards and that security is included throughout the life cycle From an examination of written software development processes, interviews of software developers, and examination of relevant data (network configuration documentation, production and test data, etc.), verify that:			
6.3.1 Testing of all security patches and system and software configuration changes before deployment	**6.3.1** All changes (including patches) are tested before being deployed into production			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
6.3.2 Separate development, test, and production environments	**6.3.2** The test/development environments are separate from the production environment, with access control in place to enforce the separation			
6.3.3 Separation of duties between development, test, and production environments	**6.3.3** There is a separation of duties between personnel assigned to the development/test environments and those assigned to the production environment			
6.3.4 Production data (live PANs) are not used for testing or development	**6.3.4** Production data (live PANs) are not used for testing and development, or are sanitized before use			
6.3.5 Removal of test data and accounts before production systems become active	**6.3.5** Test data and accounts are removed before a production system becomes active			
6.3.6 Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers	**6.3.6** Custom application accounts, usernames and/or passwords are removed before system goes into production or is released to customers			
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	**6.3.7.a** Obtain and review any written or other policies to confirm that code reviews are required and must be performed by individuals other then originating code author			
	6.3.7.b Verify code reviews are conducted for new code and after code changes *Note: This requirement applies to code reviews for custom software development, as part of the System Development Life Cycle (SDLC) – these reviews can be conducted by internal personnel. Custom code for web-facing applications will be subject to additional controls as of June 30, 2008 – see PCI DSS requirement 6.6 for details.*			
6.4 Follow change control procedures for all system and software configuration changes. The procedures must include the following:	**6.4.a** Obtain and examine company change-control procedures related to implementing security patches and software modifications, and verify that the procedures require items 6.4.1 – 6.4.4 below			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	6.4.b For a sample of system components, critical servers, and wireless access points, examine the three most recent changes/security patches for each system component, and trace those changes back to related change control documentation. Verify that, for each change examined, the following was documented according to the change control procedures:			
6.4.1 Documentation of impact	**6.4.1** Verify that documentation of customer impact is included in the change control documentation for each sampled change			
6.4.2 Management sign-off by appropriate parties	**6.4.2** Verify that management sign-off by appropriate parties is present for each sampled change			
6.4.3 Testing of operational functionality	**6.4.3** Verify that operational functionality testing was performed for each sampled change			
6.4.4 Back-out procedures	**6.4.4** Verify that back-out procedures are prepared for each sampled change			
6.5 Develop all web applications based on secure coding guidelines. such as the *Open Web Application Security Project Guidelines*. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes, to include the following:	**6.5.a** Obtain and review software development processes for any web-based applications. Verify that processes require training in secure coding techniques for developers, and are based on guidance such as the *OWASP Guidelines* (http://www.owasp.org)			
	6.5.b For any web-based applications, verify that processes are in place to confirm that web applications are not vulnerable to the following			
6.5.1 Unvalidated input	**6.5.1** Unvalidated input			
6.5.2 Broken access control (for example, malicious use of user IDs)	**6.5.2** Malicious use of User IDs			
6.5.3 Broken authentication and session management (use of account credentials and session cookies)	**6.5.3** Malicious use of account credentials and session cookies			
6.5.4 Cross-site scripting (XSS) attacks	**6.5.4** Cross-site scripting			
6.5.5 Buffer overflows	**6.5.5** Buffer overflows due to unvalidated input and other causes			
6.5.6 Injection flaws (for example,	**6.5.6** SQL injection and other command injection flaws			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
structured query language (SQL) injection)				
6.5.7 Improper error handling	**6.5.7** Error handling flaws			
6.5.8 Insecure storage	**6.5.8** Insecure storage			
6.5.9 Denial of service	**6.5.9** Denial of service			
6.5.10 Insecure configuration management	**6.5.10** Insecure configuration management			
6.6 Ensure that all web-facing applications are protected against known attacks by either of the following methods: • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application-layer firewall in front of web-facing applications *Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*	**6.6** For web-based applications, ensure that one of the following methods are in place as follows: • Verify that custom application code is periodically reviewed by an organization that specializes in application security; that all coding vulnerabilities were corrected; and that the application was re-evaluated after the corrections • Verify that an application-layer firewall is in place in front of web-facing applications to detect and prevent web-based attacks			

Implement Strong Access Control Measures

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

This requirement ensures critical data can only be accessed by authorized personnel.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.	**7.1** Obtain and examine written policy for data control, and verify that the policy incorporates the following: • Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities • Assignment of privileges is based on individual personnel's job classification and function • Requirement for an authorization form signed by management that specifies required privileges • Implementation of an automated access control system			
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	**7.2** Examine system settings and vendor documentation to verify that an access control system is implemented and that it includes the following • Coverage of all system components • Assignment of privileges to individuals based on job classification and function • Default "deny-all" setting (some access control systems are set by default to "allow-all" thereby permitting access unless/until a rule is written to specifically deny it)			

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

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 authorized users.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.1 Identify all users with a unique user name before allowing them to access system components or cardholder data.	**8.1** For a sample of user IDs, review user ID listings and verify that all users have a unique username for access to system components or cardholder data			
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: • Password • Token devices (for example, SecureID, certificates, or public key) • Biometrics	**8.2** To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder environment, perform the following: • Obtain and examine documentation describing the authentication method(s) used • For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s)			
8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	**8.3** To verify that two-factor authentication is implemented for all remote network access, observe an employee (for example, an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (Smart card, token PIN) are required.			
8.4 Encrypt all passwords during transmission and storage on all system components.	**8.4.a** For a sample of system components, critical servers, and wireless access points, examine password files to verify that passwords are unreadable			
	8.4.b For **Service Providers** only, observe password files to verify that customer passwords are encrypted			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:	**8.5** Review procedures and interview personnel to verify that procedures are implemented for user authentication and password management, by performing the following:			
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	**8.5.1.a** Select a sample of user IDs, including both administrators and general users. Verify that each user is authorized to use the system according to company policy by performing the following: • Obtain and examine an authorization form for each ID • Verify that the sampled User IDs are implemented in accordance with the authorization form (including with privileges as specified and all signatures obtained,.), by tracing information from the authorization form to the system			
	8.5.1.b Verify that only administrators have access to management consoles for wireless networks			
8.5.2 Verify user identity before performing password resets	**8.5.2** Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, email, web, or other non-face-to-face method, the user's identity is verified before the password is reset			
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use	**8.5.3** Examine password procedures and observe security personnel to verify that first-time passwords for new users are set to a unique value for each user and changed after first use			
8.5.4 Immediately revoke access for any terminated users	**8.5.4** Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been inactivated or removed			
8.5.5 Remove inactive user accounts at least every 90 days	**8.5.5** For a sample of user IDs, verify that there are no inactive accounts over 90 days old			
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	**8.5.6** Verify that any accounts used by vendors to support and maintain system components are inactive, enabled only when needed by the vendor, and monitored while being used			
8.5.7 Communicate password procedures and policies to all	**8.5.7** Interview the users from a sample of user IDs, to verify that they are familiar with password procedures and policies			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
users who have access to cardholder data				
8.5.8 Do not use group, shared, or generic accounts and passwords	**8.5.8.a** For a sample of system components, critical servers, and wireless access points, examine user ID lists to verify the following • Generic User IDs and accounts are disabled or removed • Shared User IDs for system administration activities and other critical functions do not exist • Shared and generic User IDs are not used to administer wireless LANs and devices			
	8.5.8.b Examine password policies/procedures to verify that group and shared passwords are explicitly prohibited			
	8.5.8.c Interview system administrators to verify that group and shared passwords are not distributed, even if requested			
8.5.9 Change user passwords at least every 90 days	**8.5.9** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days For **Service Providers** only, review internal processes and customer/user documentation to verify that customer passwords are required to change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change			
8.5.10 Require a minimum password length of at least seven characters	**8.5.10** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long For **Service Providers** only, review internal processes and customer/user documentation to verify that customer passwords are required to meet minimum length requirements			
8.5.11 Use passwords containing both numeric and alphabetic characters	**8.5.11** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters For **Service Providers** only, review internal processes and			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	customer/user documentation to verify that customer passwords are required to contain both numeric and alphabetic characters			
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	**8.5.12** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords For **Service Providers** only, review internal processes and customer/user documentation to verify that new customer passwords cannot be the same as the previous four passwords			
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	**8.5.13** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that a user's account is locked out after not more than six invalid logon attempts For **Service Providers** only, review internal processes and customer/user documentation to verify that customer accounts are temporarily locked-out after not more than six invalid access attempts			
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	**8.5.14** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for thirty minutes or until a system administrator resets the account			
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	**8.5.15** For a sample of system components, critical servers, and wireless access points, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less			
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	**8.5.16.a** Review database configuration settings for a sample of databases to verify that access is authenticated, including for individual users, applications, and administrators			
	8.5.16.b Review database configuration settings and database accounts to verify that direct SQL queries to the database are prohibited (there should be very few individual database login accounts. Direct SQL queries should be limited to database administrators)			

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use			
9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	**9.1.1** Verify that video cameras monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Verify that cameras are monitored and that data from cameras is stored for at least three months			
9.1.2 Restrict physical access to publicly accessible network jacks	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks			
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	**9.1.3** Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted			
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *"Employee" refers to full-time and part-time employees, temporary*	**9.2.a** Review processes and procedures for assigning badges to employees, contractors, and visitors, and verify these processes include the following: • Procedures in place for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges • Limited access to badge system			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
employees and personnel, and consultants who are "resident" on the entity's site. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.	**9.2.b** Observe people within the facility to verify that it is easy to distinguish between employees and visitors			
9.3 Make sure all visitors are handled as follows:	**9.3** Verify that employee/visitor controls are in place as follows:			
9.3.1 Authorized before entering areas where cardholder data is processed or maintained	**9.3.1** Observe visitors to verify the use of visitor ID badges. Attempt to gain access to the data center to verify that a visitor ID badge does not permit unescorted access to physical areas that store cardholder data			
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees	**9.3.2** Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors/outsiders and that visitor badges expire			
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	**9.3.3** Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration			
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.	**9.4.a** Verify that a visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted			
	9.4.b Verify that the log contains the visitor's name, the firm represented, and the employee authorizing physical access, and is retained for at least three months			
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.	**9.5** Verify that the storage location for media backups is secure. Verify that offsite storage is visited periodically to determine that backup media storage is physically secure and fireproof			
9.6 Physically secure all paper and electronic media (including computers, electronic media, networking and communications	**9.6** Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media in computer rooms and data centers (including paper receipts, paper reports, faxes, CDs, and disks in employee desks and open			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder data	workspaces, and PC hard drives)			
9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data: including the following	**9.7** Verify that a policy exists to control distribution of media containing cardholder data, that the policy covers all distributed media including that distributed to individuals			
9.7.1 Classify the media so it can be identified as confidential	**9.7.1** Verify that all media is classified so that it can be identified as "confidential"			
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	**9.7.2** Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery mechanism that can be tracked			
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	**9.8** Select a recent sample of several days of offsite media tracking logs, and verify the presence in the logs of tracking details and proper management authorization			
9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.	**9.9** Obtain and examine the policy for controlling storage and maintenance of hardcopy and electronic media and verify that the policy requires periodic media inventories.			
9.9.1 Properly inventory all media and make sure it is securely stored.	**9.9.1.a** Obtain and review the media inventory log to verify that periodic media inventories are performed **9.9.1.b** Review processes to verify that media is securely stored			
9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows	**9.10** Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:			
9.10.1 Cross-cut shred, incinerate, or pulp hardcopy materials	**9.10.1.a** Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped, in accordance with ISO 9564-1 or ISO 11568-3e			
	9.10.1.b Examine storage containers used for information to be destroyed to verify that the containers are secured. For example, verify that a "to-be-shredded" container has a lock preventing access			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	to its contents			
9.10.2 Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed	**9.10.2** Verify that electronic media is destroyed beyond recovery by using a military wipe program to delete files, or via degaussing or otherwise physically destroying the media			

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
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.	**10.1** Verify through observation and interviewing the system administrator, that audit trails are enabled and active, including for any connected wireless networks.			
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**10.2** Verify though interviews, examination of audit logs, and examination of audit log settings, that the following events are logged into system activity logs:			
10.2.1 All individual accesses to cardholder data	**10.2.1** All individual access to cardholder data			
10.2.2 All actions taken by any individual with root or administrative privileges	**10.2.2** Actions taken by any individual with root or administrative privileges			
10.2.3 Access to all audit trails	**10.2.3** Access to all audit trails			
10.2.4 Invalid logical access attempts	**10.2.4** Invalid logical access attempts			
10.2 5 Use of identification and authentication mechanisms	**10.2.5** Use of identification and authentication mechanisms			
10.2.6 Initialization of the audit logs	**10.2.6** Initialization of audit logs			
10.2.7 Creation and deletion of system-	**10.2.7** Creation and deletion of system level objects			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
level objects				
10.3 Record at least the following audit trail entries for all system components for each event:	**10.3** Verify through interviews and observation, for each auditable event (from 10.2), that the audit trail captures the following:			
10.3.1 User identification	**10.3.1** User identification			
10.3.2 Type of event	**10.3.2** Type of event			
10.3.3 Date and time	**10.3.3** Date and time stamp			
10.3.4 Success or failure indication	**10.3.4** Success or failure indication, including those for wireless connections			
10.3.5 Origination of event	**10.3.5** Origination of event			
10.3.6 Identity or name of affected data, system component, or resource	**10.3.6** Identity or name of affected data, system component, or resources			
10.4 Synchronize all critical system clocks and times	**10.4** Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system-parameter settings for a sample of system components, critical servers, and wireless access points. Verify the following is included in the process and implemented:			
	10.4.a Verify that NTP or similar technology is used for time synchronization			
	10.4.b Verify that internal servers are not all receiving time signals from external sources. [Two or three central time servers within the organization receive external time signals [directly from a special radio, GPS satellites, or other external sources based on International Atomic Time and UTC (formerly GMT)], peer with each other to keep accurate time, and share the time with other internal servers.]			
	10.4.c Verify that the Network Time Protocol (NTP) is running the most recent version			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
	10.4.d Verify that specific external hosts are designated from which the time servers will accept NTP time updates (to prevent an attacker from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the NTP service (to prevent unauthorized use of internal time servers). See www.ntp.org for more information			
10.5 Secure audit trails so they cannot be altered	**10.5** Interview system administrator and examine permissions to verify that audit trails are secured so that they cannot be altered as follows:			
10.5.1 Limit viewing of audit trails to those with a job-related need	**10.5.1** Verify that only individuals who have a job-related need can view audit trail files			
10.5.2 Protect audit trail files from unauthorized modifications	**10.5.2** Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation			
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	**10.5.3** Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter			
10.5.4 Copy logs for wireless networks onto a log server on the internal LAN	**10.5.4** Verify that logs for wireless networks are offloaded or copied onto a centralized internal log server or media that is difficult to alter			
10.5.5 Use file integrity monitoring and 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)	**10.5.5** Verify the use of file integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities			
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	**10.6.a** Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
accounting protocol (AAA) servers (for example, RADIUS). *Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6*	**10.6.b** Through observation and interviews, verify that regular log reviews are performed for all system components			
10.7 Retain audit trail history for at least one year, with a minimum of three months available online.	**10.7.a** Obtain and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year			
	10.7.b Verify that audit logs are available online or on tape for at least one year			

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by hackers and researchers, and being introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.	**11.1.a** Confirm by interviewing security personnel and examining relevant code, documentation, and processes that security testing of devices is in place to assure that controls identify and stop unauthorized access attempts within the cardholder environment.			
	11.1.b Verify that a wireless analyzer is used at least quarterly to identify all wireless devices.			
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).	**11.2.a** Inspect output from the most recent four quarters of network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Verify that the scan process includes rescans until "clean" results are obtained			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
Note: Quarterly external vulnerability scans must be performed by a scan vendor qualified by the payment card industry. Scans conducted after network changes may be performed by the company's internal staff.	**11.2.b** To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify that • Four quarterly scans occurred in the most recent 12-month period • The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities) • The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures			
11.3 Perform 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	**11.3** Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment. Verify that any noted vulnerabilities were corrected. Verify that the penetration tests include:			
11.3.1 Network-layer penetration tests	**11.3.1** Network-layer penetration tests			
11.3.2 Application-layer penetration tests	**11.3.2** Application-layer penetration tests			
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.	**11.4.a** Observe the use of network intrusion detection systems and/or intrusion prevention systems on the network. Verify that all critical network traffic in the cardholder data environment is monitored			
	11.4.b Confirm IDS and/or IPS is in place to monitor and alert personnel of suspected compromises			
	11.4.c Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly. *Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider)*	**11.5** Verify the use of file integrity monitoring products within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities			

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	**12.1** Examine the information security policy and verify that the policy is published and disseminated to all relevant system users (including vendors, contractors, and business partners)			
12.1.1 Addresses all requirements in this specification	**12.1.1** Verify that the policy addresses all requirements in this specification.			
12.1.2 Includes an annual process	**12.1.2** Verify that the information security policy includes			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
that identifies threats, and vulnerabilities, and results in a formal risk assessment	an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment			
12.1.3 Includes a review at least once a year and updates when the environment changes	**12.1.3** Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment			
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).	**12.2.a** Examine the daily operational security procedures. Verify that they are consistent with this specification, and include administrative and technical procedures for each of the requirements			
12.3 Develop usage policies for critical employee-facing technologies (such as modems and wireless) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	**12.3** Obtain and examine the policy for critical employee-facing technologies and verify the policy contains the following:			
12.3.1 Explicit management approval	**12.3.1** Verify that the usage policies require explicit management approval to use the devices			
12.3.2 Authentication for use of the technology	**12.3.2** Verify that the usage policies require that all device use is authenticated with username and password or other authentication item (for example, token)			
12.3.3 A list of all such devices and personnel with access	**12.3.3** Verify that the usage policies require a list of all devices and personnel authorized to use the devices			
12.3.4 Labeling of devices with owner, contact information, and purpose	**12.3.4** Verify that the usage policies require labeling of devices with owner, contact information, and purpose			
12.3.5 Acceptable uses of the technology	**12.3.5** Verify that the usage policies require acceptable uses for the technology			
12.3.6 Acceptable network locations for the technologies	**12.3.6** Verify that the usage policies require acceptable network locations for the technology			
12.3.7 List of company-approved products	**12.3.7** Verify that the usage policies require a list of company-approved products			
12.3.8 Automatic disconnect of	**12.3.8** Verify that the usage policies require automatic			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
modem sessions after a specific period of inactivity	disconnect of modem sessions after a specific period of inactivity			
12.3.9 Activation of modems for vendors only when needed by vendors, with immediate deactivation after use	**12.3.9** Verify that the usage policies require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use			
12.3.10 When accessing cardholder data remotely via modem, prohibition of storage of cardholder data onto local hard drives, floppy disks, or other external media. Prohibition of cut-and-paste and print functions during remote access	**12.3.10** Verify that the usage policies prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem. Verify that the policies prohibit cut-and-paste and print functions during remote access			
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.	**12.4** Verify that information security policies clearly define information security responsibilities for both employees and contractors			
12.5 Assign to an individual or team the following information security management responsibilities:	**12.5** Verify the formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. Obtain and examine information security policies and procedures to verify that the following information security responsibilities are specifically and formally assigned:			
12.5.1 Establish, document, and distribute security policies and procedures	**12.5.1** Verify that responsibility for creating and distributing security policies and procedures is formally assigned			
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel	**12.5.2** Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned			
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations	**12.5.3** Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned			
12.5.4 Administer user accounts,	**12.5.4** Verify that responsibility for administering user			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
including additions, deletions, and modifications	account and authentication management is formally assigned			
12.5.5 Monitor and control all access to data	**12.5.5** Verify that responsibility for monitoring and controlling all access to data is formally assigned			
12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security:	**12.6.a** Verify the existence of a formal security awareness program for all employees			
	12.6.b Obtain and examine security awareness program procedures and documentation and perform the following:			
12.6.1 Educate employees upon hire and at least annually (for example, by letters, posters, memos, meetings, and promotions)	**12.6.1.a** Verify that the security awareness program provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)			
	12.6.1.b Verify that employees attend awareness training upon hire and at least annually			
12.6.2 Require employees to acknowledge in writing that they have read and understood the company's security policy and procedures	**12.6.2** Verify that the security awareness program requires employees to acknowledge in writing that they have read and understand the company's information security policy			
12.7 Screen potential employees to minimize the risk of attacks from internal sources. *For those employees 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.*	**12.7** Inquire of Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential employees who will have access to cardholder data or the cardholder data environment. (Examples of background checks include pre-employment, criminal, credit history, and reference checks)			
12.8 If cardholder data is shared with service providers, then contractually the following is required:	**12.8** If the audited entity shares cardholder data with another company, obtain and examine contracts between the organization and any third parties that handle cardholder data (for example, backup tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes). Perform the following:			
12.8.1 Service providers must	**12.8.1** Verify that the contract contains provisions requiring			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
adhere to the PCI DSS requirements	adherence to the PCI DSS requirements			
12.8.2 Agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses	**12.8.2** Verify that the contract contains provisions for acknowledgement by the third party of their responsibility for securing cardholder data			
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**12.9** Obtain and examine the Incident Response Plan and related procedures and perform the following:			
12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing the Acquirers and credit card associations)	**12.9.1** Verify that the Incident Response Plan and related procedures include • roles, responsibilities, and communication strategies in the event of a compromise • coverage and responses for all critical system components • notification, at a minimum, of credit card associations and acquirers • strategy for business continuity post compromise • reference or inclusion of incident response procedures from card associations • analysis of legal requirements for reporting compromises (for example, per California bill 1386, notification of affected consumers is a requirement in the event of an actual or suspected compromise, for any business with California residents in their database)			
12.9.2 Test the plan at least annually	**12.9.2** Verify that the plan is tested at least annually			
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts	**12.9.3** Verify through observation and review of policies, that there is 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, critical IDS alerts, and/or reports of unauthorized critical system or content file changes			
12.9.4 Provide appropriate training to staff with security breach	**12.9.4** Verify through observation and review of policies that staff with security breach responsibilities are			

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
response responsibilities	periodically trained			
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems	**12.9.5** Verify through observation and review of processes that monitoring and responding to alerts from security systems are included in the Incident Response Plan			
12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments	**12.9.6** Verify through observation and review of policies that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments			
12.10 All processors and service providers must maintain and implement policies and procedures to manage connected entities, to include the following	**12.10** Verify through observation, review of policies and procedures, and review of supporting documentation that there is a process to manage connected entities by performing the following:			
12.10.1 Maintain list of connected entities	**12.10.1** Verify that a list of connected entities is maintained			
12.10.2 Ensure proper due diligence is conducted prior to connecting an entity	**12.10.2** Verify that procedures ensure that proper due diligence is conducted prior to connecting an entity			
12.10.3 Ensure the entity is PCI DSS compliant	**12.10.3** Verify that procedures ensure that the entity is PCI DSS compliant			
12.10.4 Connect and disconnect entities by following an established process	**12.10.4** Verify that connecting and disconnecting entities occurs following an established process			

Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)

Requirement A.1: Hosting providers protect cardholder data environment

As referenced in Requirement 12.8, all service providers with access to cardholder data (including hosting providers) must adhere to the PCI DSS. In addition, Requirement 2.4 states that hosting providers must protect each entity's hosted environment and data. Therefore, hosting providers must give special consideration to the following::

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
A.1 Protect each entity's (that is merchant, service provider, or other entity) hosted environment and data, as in 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. *Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity* must *comply with the PCI DSS and validate compliance as applicable.*	**A.1** Specifically for a PCI audit of a **Shared hosting Provider**, to verify that **Shared hosting Providers** protect entities' (merchants and service providers) hosted environment and data, select a sample of servers (Microsoft Windows and Unix/Linux) across a representative sample of hosted merchants and service providers, and verify **A.1.1** through **A.1.4** below.			
A.1.1 Ensure that each entity only has access to own cardholder data environment	**A.1.1** If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: • No entity on the system can use a shared web server user ID • All CGI scripts used by an entity must be created and run as the entity's unique user ID			
A.1.2 Restrict each entity's access and privileges to own cardholder	**A.1.2.a** Verify the user ID of any application process is not a privileged user (root/admin).			

Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
	A.1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). IMPORTANT: An entity's files may not be shared by group			
	A.1.2.c Verify an entity's users do not have write access to shared system binaries			
	A.1.2.d Verify that viewing of log entries is restricted to the owning entity			
	A.1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities (error, race, and restart conditions, resulting in, for example, buffer overflows), verify restrictions are in place for the use of these system resources: • Disk space • Bandwidth • Memory • CPU			
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	**A.1.3.a** Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: • Logs are enabled for common third party applications • Logs are active by default • Logs are available for review by the owning entity • Log locations are clearly communicated to the owning entity			
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	**A.1.4** Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.			

Appendix B – Compensating Controls

Compensating Controls – General

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a technical specification of a requirement, but has sufficiently mitigated the associated risk. See the PCI DSS Glossary for the full definition of compensating controls.

The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments. Each compensating control must be thoroughly evaluated after implementation to ensure effectiveness. The following guidance provides compensating controls when companies are unable to render cardholder data unreadable per requirement 3.4.

Compensating Controls for Requirement 3.4

For companies unable to render cardholder data unreadable (for example, by encryption) due to technical constraints or business limitations, compensating controls may be considered. *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the "Compensating Controls" definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet **all of the** following conditions:

1. Provide additional segmentation/abstraction (for example, at the network-layer)
2. Provide ability to restrict access to cardholder data or databases based on the following criteria:
    - IP address/Mac address
    - Application/service
    - User accounts/groups
    - Data type (packet filtering)
3. Restrict logical access to the database
    - Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP)
4. Prevent/detect common application or database attacks (for example, SQL injection).

Appendix C: Compensating Controls Worksheet/Completed Example

Example

1. Constraints: List constraints precluding compliance with the original requirement

Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a 'root' login. It is not possible for Company XYZ to manage the 'root' login nor is it feasible to log all 'root' activity by each user.

2. Objective: Define the objective of the original control; identify the objective met by the compensating control

The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, shared logins makes it impossible to state definitively that a person is responsible for a particular action.

3. Identified Risk: Identify any additional risk posed by the lack of the original control

Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.

4. Definition of Compensating Controls: Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.

Company XYZ is going to require all users to log into the servers from their desktop using the SU command. SU allows a user to access the 'root' account and perform actions under the 'root' account but is able to be logged in the su-log directory. In this way, each user's actions can be tracked through the SU account.