PCI DSS
Self Assessment Questionnaire (SAQ) Tool
&
Compliance Attestation Documentation

Developed and Provided Through The Reymann Group

CONTENTS

Purpose of this Tool:

The following template is provided as an easy way for merchants to use the WatchGuard solution and other technologies and processes to deliver continuous compliance with the PCI DSS requirements.

JANUARY 2009

PCI DSS SELF ASSESSMENT QUESTIONNAIRE (SAQ) TOOL & COMPLIANCE ATTESTATION DOCUMENTATION

This Document:

☑ Automates and streamlines the self-assessment process and monthly attestation process.

☑ Includes all of the PCI DSS self-assessment questions and applicable testing procedures.

☑ Aligns each of the PCI DSS self-assessment questions against the specific WatchGuard solution capabilities, where applicable.

☑ Provides a space for customers to fill in the non WatchGuard requirements.

☑ Can serve as supporting documentation for the merchant's monthly attestation of PCI DSS compliance.

WatchGuard supplies a matching report or reports for validating and testing several of these controls in a standardized format that can be printed each month and attached to the attestation report. It can also be used in the event that customers must prove compliance to an internal or external auditor or as forensic follow-up resulting from a material event.

PCI DSS Self Assessment Tool and Supporting Attestation Documentation

HOW TO GET THE MOST VALUE FROM THIS TOOL:

- Step 1: Download the SAQ Tool online at the WatchGuard website.
- Step 2: Read each question and test procedure carefully and select YES or NO for each question, as appropriate. WatchGuard has already provided the necessary information where the WatchGuard UTM appliance solution is deployed.
- Step 3: Save the final results and print a copy of the report as the completed report for submission (in hard copy or electronic PDF) as the company's monthly self-assessment and attestation for PCI DSS compliance to the Merchant Acquire Bank.

Build and Maintain a Secure Network *Requirement 1: Install and maintain a firewall configuration to protect data*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on firewall configurations and other like systems outside of the WatchGuard capabilities.			
1.1	Do established firewall configuration standards include the following? Test Procedure: Obtain and inspect the firewall and router configuration standards and other documentation specified below to very that standards are complete.		
1.1.1	A formal process for approving and testing all external network connections and changes to the firewall and router configuration?	□	□
	Test Procedure: Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.		
1.1.2	A current network diagram with all connections to cardholder data, including any wireless networks?	□	□
	Test Procedure: a. Verify that a current network diagram (e.g., one that shows cardholder data flows over the network) exists and that it documents all connections to cardholder data, including any wireless networks. 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?	□	□
	Test Procedure: Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. 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?	□	□
	Test Procedure: Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.		
1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure?	□	□
	Test Procedure: a. Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business – e.g., hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols. b. Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.		
1.1.6	Requirement to review firewall and router rule sets at least every six months?	□	□
	Test Procedure: a. Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. b. Obtain and examine documentation to verify that the rule sets are reviewed at least every six months.		
1.2	Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder environment? *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, or which is out of the entity's ability to control or manage.*	□	□

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect data

	Question	**Yes**	**No**
	Test Procedure: Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment.		
	The Firebox Proxy architecture is ideal for meeting these requirements. The Proxy architecture provides detailed control over which protocols, ports and content are allowed through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy that allows only approved traffic to pass into the cardholder data environment. The Firebox IPS and AV services can also be used to scan the allowed traffic to monitor for threats from malware or unauthorized intrusion attempts.		
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?	□	□
	Test Procedure: a. Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented. b. Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "demy all" or an implicit deny after allow statement		
	The Firebox Proxy architecture provides granular control over which protocols, ports and content are allowed through the firewall. Using the Firebox Proxy technology will block ALL traffic except for that explicitly defined by the user.		
1.2.2	Secure and synchronize router configuration files?	□	□
	Test Procedure: 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.		
	This requirement only affects a Firebox if used as primary router. If this is the case, then the WatchGuard System Manager may be used to define and deploy a synchronized configuration to each Firebox that will then be applied during the startup of each appliance.		
1.2.3	Include installation of perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment?	□	□
	Test Procedure: 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 the cardholder data environment.		
	If using a Firebox Core or Peak: • Using port independence, an interface can be assigned to the Wireless Access Point (WAP) and policies defined to ensure that no traffic from the WAP is allowed to enter the cardholder data environment. If using a Firebox Edge as the WAP: • The Edge can be configured so that the wireless traffic is isolated from the cardholder data environment via firewall policy.		
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?	□	□
	Test Procedure: Examine firewall and router configurations, as detailed below, to determine that there is no direct access between the Internet and system components, including the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment.		

Build and Maintain a Secure Network *Requirement 1: Install and maintain a firewall configuration to protect data*			
	Question	**Yes**	**No**
	This relates specifically to the use of a “zoned” network architecture to prevent direct access to the cardholder data environment from the Internet. A zoned network is one that is grouped into subnets, with each segment set aside for a specific function or IP Range. At a minimum, a PCI DSS network is segregated into two subnets; a demilitarized zone (or DMZ) for the public facing servers and the cardholder data environment (or “trusted” zone). Public facing servers placed into the DMZ subnet protect the cardholder data environment in case an intruder succeeds in penetrating them. An intervening firewall controls the traffic between the DMZ servers and the internal network clients. Firebox appliances can be used as the intervening firewall, establishing the subnets for each zone and controlling the traffic that passes from one zone to another.		
1.3.1	Is the DMZ implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder environment?	□	□
	Test Procedure: Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.		
	To match the requirements for this section, a Firebox must be configured to create a DMZ for all public facing servers and a “Trusted” zone for the cardholder data environment. Proxy policies are then used to provide detailed control over which protocols, ports and content are allowed into and out of each zone.		
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	□	□
	Test Procedure: Verify that inbound Internet traffic is limited to IP addresses within the DMZ.		
	With a Firebox in a “zoned” network configuration, all traffic passed between the Internet and the internal network can only go to and from servers at public facing IP addresses within the DMZ, prohibiting any direct routes for either inbound or outbound Internet traffic to the cardholder data environment.		
1.3.3	Are direct routes prohibited for inbound and outbound traffic between the Internet and the cardholder data environment?	□	□
	Test Procedure: Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.		
	With a Firebox in a “zoned” network configuration, all traffic passed between the Internet and the internal network can only go to and from servers at public facing IP addresses within the DMZ, prohibiting any direct routes for either inbound or outbound Internet traffic to the cardholder data environment.		
1.3.4	Are internal addresses prohibited from passing from the Internet to the DMZ?	□	□
	Test Procedure: Verify that internal addresses cannot pass from the Internet into the DMZ.		
	A Firebox in a “zoned” network configuration ensures that: • All incoming traffic from the Internet not destined for a public IP address in the DMZ is denied.		
1.3.5	Is outbound traffic restricted from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ?	□	□
	Test Procedure: Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.		
	A Firebox in a “zoned” network configuration ensures that: • All traffic FROM the cardholder data environment going to an IP address not within the DMZ is denied, ensuring that all data FROM the cardholder data environment cannot be routed directly to the Internet.		
1.3.6	Is stateful inspection, also know as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?	□	□

Build and Maintain a Secure Network *Requirement 1: Install and maintain a firewall configuration to protect data*			
	Question	**Yes**	**No**
	Test Procedure: 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 a port scanner 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).]		
	The Proxy technology used in Firebox appliances go beyond basic stateful inspection and also incorporate other technologies, such as Protocol Anomaly Detection and Intrusion Prevention Services that can be used to meet or exceed the objectives of this requirement.		
1.3.7	Is the database placed in an internal network zone, segregated from the DMZ?	□	□
	Test Procedure: Verify that the database is on and internal network zone is segregated from the DMZ.		
1.3.8	Has IP-masquerading been implemented to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space?	□	□
	Test Procedure: For the sample of firewall and router components, 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).		
	With dynamic NAT, the Firebox replaces the private IP address included in a packet sent from a computer protected by the Firebox with the public IP address of the Firebox itself. By default, dynamic NAT is enabled and active for RFC 1918 private network addresses.		
1.4	Has personal firewall software been installed on any mobile or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization’s network?	□	□
	Test Procedure: a. Verify that mobile and employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), and which are used to access the organization’s network, have personal firewall software installed and active. b. Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by mobile computer uses.		

Build and Maintain a Secure Network *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on vendor supplied defaults for system passwords and other security parameters outside of the WatchGuard capabilities.			
2.1	Are vendor-supplied defaults changed **before** installing a system on the network? *(Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.)*	□	□
	Test Procedure: 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 and passwords.)		
2.1.1	Are defaults** for wireless environments connected to the cardholder data environment or transmitting cardholder data changed before installing a wireless system? Are wireless device security settings enabled for strong encryption technology for authentication and transmissions? *** Such wireless environment defaults include but are not limited to, default wireless encryption keys, passwords, and SNMP community strings.*	□	□
	Test Procedure: Verify the following regarding vendor default settings for wireless environments and ensure that all wireless networks implement strong encryption mechanisms (for example AES): a. Encryption keys were changed from default at installation and are changed at anytime anyone with knowledge of the keys leaves the company or changes positions. b. Default SNMP community strings on wireless devices were changed. c. Default passwords/passphrases on access points were changed. d. Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks (for example, WPA/WPA2). e. Other security-related wireless vendor defaults, if applicable.		
2.2.a	Have configuration standards been developed for all system components? Do these standards address all known security vulnerabilities and are they consistent with industry-accepted system hardening standards – e.g., by SysAdmin Audit Network Security Networks (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)?	□	□
	Test Procedure: a. Examine the organization’s system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards - e.g., SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security(CIS). b. Verify that system configuration standards are applied when new systems are configured.		
2.2.b	Do controls ensure the following?		
2.2.1	Is only one primary function implemented per server?	□	□
	Test Procedure: For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.		
2.2.2	Do controls ensure that all unnecessary and insecure services and protocols are disabled (services and protocols not directly needed to perform the devices’ specified function)?	□	□
	Test Procedure: For a sample of system components, 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.		

Build and Maintain a Secure Network *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*			
	Question	**Yes**	**No**
	Firebox appliances' Proxy architecture provides detailed control over which protocols, ports and content are allowed passage through the firewall. This is achieved by blocking all traffic by default and defining a proxy policy for those specific protocols that are allowed.		
2.2.3	Do controls ensure that system parameters are configured to prevent misuse?	🟩 □	□
	Test Procedure: a. Interview system administrators and security managers to verify that they have knowledge of common security parameter settings for system components. b. Verify that common security parameter settings are included in the system configuration standards. c. For a sample of system components, verify that common security parameters are set appropriately.		
	Firebox configuration can only be achieved through the use of Administrative pass phrases. Different pass phrases are required for reading and writing Firebox configurations to the appliance.		
2.2.4	Has all unnecessary functionality – such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers – been removed?	□	□
	Test Procedure: For a sample of system components, verify that all unnecessary functionality (e.g., scripts, drivers, features, subsystems, file systems, etc.) is removed. Verify enabled functions are documented and support secure configuration and that only documented functionality is present on the sample machines.		
2.3	Is all non-console administrative access encrypted? *Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.*	🟩 □	□
	Test Procedure: For a sample of system components, verify that non-console administrative access is encrypted by: a. Observing an administrator log on to each system to verify that a strong encryption method is involved before the administrator's password is requested. b. Reviewing services and parameter files on systems to determine that Telnet and other remote log-in commands are not available for use internally. c. Verifying that administrator access to the web-based management interfaces is encrypted with strong cryptography.		
	All management communications with Firebox appliances are done via a secure encryption-based protocol.		
2.4	If you are a hosting provider, are your systems configured to protect each entity's hosted environment and cardholder data?	□	□

Build and Maintain a Secure Network *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*			
	Question	**Yes**	**No**
	<u>Test Procedure</u>: Perform testing procedures A.1.1 through A.1.4 detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers* for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data. A.1.1 - If a shared hosting provider allows entities (e.g., merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity. For example: a. No entity on the system can use a shared web server user ID. b. All CGI scripts used by an entity must be created and run as the entity's unique user ID. A.1.2 – Verify: a. The user ID of any application process is not a privileged user (root/admin). b. 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. c. An entity's users do not have write access to shared system binaries. d. Viewing of log entries is restricted to the owning entity. e. Restrictions are in place for the user of these system resources: disk space; bandwidth; memory; and CPU. This is to ensure that each entity cannot monopolize server resources to exploit vulnerabilities (e.g., error, race, and restart conditions, resulting in, for example, buffer overflows). A.1.3 - Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: a. Logs are enabled for common third-party applications. b. Logs are active by default. c. Logs are available for review by the owning entity. d. Log locations are clearly communicated to the owning entity. 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.		

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

	Question	Yes	No
	In addition to the WatchGuard capabilities, additional reviews should be performed on protection of stored cardholder data outside of the WatchGuard capabilities.		
3.1	Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and regulatory purposes? Is there a data-retention and disposal policy, and does it include such limitations?	□	□
	<u>Test Procedure</u>: Obtain and examine the company policies and procedures for data retention and disposal and verify that policies and procedures include: a. Legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data(e.g., cardholder data needs to be held for X period for Y business reasons). b. Provisions for disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data. c. Coverage for all storage of cardholder data. d. A programmatic (automatic) process to remove, at least on a quarterly basis, stored cardholder data that exceeds business retention requirements, or alternatively, requirements for a review that is conducted at least on a quarterly basis to verify that stored cardholder data does not exceed business retention requirements.		
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authentication (even if encrypted)?	□	□
	<u>Test Procedure</u>: If sensitive authentication data is received and deleted, obtain and review the processes for deleting the data to verify that the data is unrecoverable.		
3.2.1	Do not store the full contents of any track from the magnetic stripe (located 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 cardholder's name, primary account number (PAN), expiration date, and service code. To minimize risk, store only those data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements.*	□	□
	<u>Test Procedure</u>: For a sample of system components, examine the following and verify the full contents of any track from the magnetic stripe on the back of card are not stored under any circumstance: a. Incoming transaction data b. All logs(e.g., transaction, history, debugging, error) c. History files d. Trace files e. Several database schemas f. Database contents		
3.2.2	Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	□	□

Protect Cardholder Data *Requirement 3: Protect stored cardholder data*			
	Question	**Yes**	**No**
	Test Procedure: For a sample of system components, verify that the three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored under any circumstance: a. Incoming transaction data b. All logs (e.g., transaction, history, debugging, error) c. History files d. Trace file e. Several database schemas f. Database contents		
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	□	□
	Test Procedure: For a sample of system components, examine the following and verify that PINs and encrypted PIN blocks are not stored under any circumstances: a. Incoming transaction data b. All logs (e.g., transaction, history, debugging, error) c. History files d. Trace file e. Several database schemas f. Database contents		
3.3	Is the PAN masked 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 (e.g., for point-of-sale (POS) receipts).*	□	□
	Test Procedure: Obtain and examine written policies and examine displays of PAN (e.g., on screen, on paper receipts) to verify that primary account numbers (PANs) are masked when displaying cardholder data, except for those with a legitimate business need to see full PAN.		
3.4	Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, back-up media, and in logs,) by using any of the following approaches? – One-way hashes based on strong cryptography – 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 render the PAN unreadable, refer to “Compensating Controls.”*	□	□

Protect Cardholder Data *Requirement 3: Protect stored cardholder data*			
	Question	**Yes**	**No**
	<u>Test Procedure</u>: a. Obtain and examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods: – One-way hashes based on strong cryptography. – Truncation. – Index tokens and pads with the pads being securely stored. – Strong cryptography with associated key-management processes and procedures. b. Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). c. Examine a sample of removable media (e.g., back-up tapes) to confirm that the PAN is rendered unreadable. d. Examine a sample of audit logs to confirm that the PAN is sanitized or removed from the logs.		
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used:		
3.4.1.a	Is logical access managed independently of native operating system access control mechanisms (e.g., by not using local user account databases)?	□	□
	<u>Test Procedure</u>: 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 (e.g., not using local user account databases).		
3.4.1.b	Are decryption keys independent of user accounts?	□	□
	<u>Test Procedure</u>: a. Verify that cryptographic keys are stored securely (e.g., stored on removable media that is adequately protected with strong access controls). b. Verify that cardholder data on removable media is encrypted wherever stored. *Note: Disk encryption often cannot encrypt removable media, so data stored on this media will need to be encrypted separately.*		
3.5	Are encryption keys used for encryption of cardholder data protected against both disclosure and misuse?	□	□
	<u>Test Procedure</u>: Verify processes to protect keys used for encryption of cardholder data against disclosure and misuse by performing the following.		
3.5.1	Is access to cryptographic keys restricted to the fewest number of custodians necessary?	□	□
	<u>Test Procedure</u>: Examine user access lists to verify that access to keys is restricted to very few custodians.		
3.5.2	Are cryptographic keys stored securely and in the fewest possible locations and forms?	□	□
	<u>Test Procedure</u>: Examine system configuration files to verify that keys are stored in encrypted format and that key-encrypting keys are stored separately from data-encrypting keys.		
3.6	Are all key-management processes ad procedures for cryptographic keys used for encryption of cardholder data fully documented and implemented? Do they include the following:	□	□
	<u>Test Procedure</u>: a. Verify the existence for key-management procedures for keys used for encryption of cardholder data. *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.* 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 keys (used t transmit data between customer and service provider).		

Protect Cardholder Data
Requirement 3: Protect stored cardholder data

	Question	Yes	No
3.6.1	Generation of strong cryptographic keys?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require the generation of strong keys.		
3.6.2	Secure cryptographic key distribution?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require secure key distribution.		
3.6.3	Secure cryptographic key storage?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require secure key storage.		
3.6.4	Periodic changing of cryptographic keys? – As deemed necessary and recommended by the associated application (e.g., re-keying); preferably automatically, and – At least annually.	□	□
	Test Procedure: Verify that key-management procedures are implemented to require periodic key changes at least annually.		
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys?	□	□
	Test Procedure: a. Verify that key management procedures are implemented to require the retirement of old keys (e.g., archiving, destruction, and revocation as applicable). b. Verify that key-management procedures are implemented to require the replacement of known or suspected compromised keys.		
3.6.6	Split knowledge and establishment of dual control of cryptographic keys?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require split knowledge and dual control of keys (e.g., requiring two or more people, each knowing only their own part of the key, to reconstruct the whole key.)		
3.6.7	Prevention of unauthorized substitution of cryptographic keys?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require the prevention of unauthorized substitution of keys.		
3.6.8	Requirements for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities?	□	□
	Test Procedure: Verify that key-management procedures are implemented to require key custodians to sign a form specifying that they understand and accept their key-custodian responsibilities.		

Protect Cardholder Data *Requirement 4: Encrypt transmission of cardholder data across open, public networks*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on protection of cardholder data while in transit outside of the WatchGuard capabilities.			
4.1	Are strong cryptograph and security protocols, such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC), used 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; wireless technologies; global system for mobile communications (GSM); and general packet radio service (GPRS).)*	[✓ □]	□
	<u>Test Procedure:</u> Verify the use of encryption (e.g., SSL/TLS or IPSEC) wherever cardholder data is transmitted or received over open, public networks. a. Verify that strong encryption is used during data transmission. b. For SSL implementations: – Verify that the server supports the latest patched versions. – Verify that HTTPS appears as a part of the browser Universal Record Locator (URL). – Verify that no card holder data is required when HTTPS does not appear in the URL. c. Select a sample of transactions as they are received and observe transactions as they occur to verify that cardholder data is encrypted during transit. d. Verify that only trusted SSL/TLS keys/certificates are accepted. e. Verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommended best practices.)		
	All e-Series Firebox appliances running Version 10 firmware support IPSec and SSL VPN communication.		
4.1.1	Are industry best practices (e.g., IEEE 802.11i) used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment? *Notes:* – *For new wireless implementations, it is prohibited to implement WEP after Marcy 31, 2009.* – *For current wireless implementations, it s prohibited to use WEP after June 30, 2010.*	[✓ □]	□
	<u>Test Procedure:</u> For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.		
	Wireless networks are inherently insecure, but there are some circumstances where they cannot be avoided. In these cases, the standard requires that the wireless operating environment be physically segregated from the wired environment and appropriately firewalled. When a Wi-Fi solution must be used, the Edge series supports WPA2 and can be combined with either an IPSEC or SSL VPN to achieve the objectives of this requirement.		
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (e.g., e-mail, instant messaging, and chat)?	□	□
	<u>Test Procedure:</u> a. Verify that strong cryptography is used whenever cardholder data is sent via end-use messaging technologies. b. Verify the existence of a policy stating that unencrypted PANs are not to be sent via end-user messaging technologies.		

Maintain a Vulnerability Management Program *Requirement 5: Use and regularly update anti-virus software and programs*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on anti-virus software and programs outside of the WatchGuard capabilities.			
5.1	Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?	□	□
	Test Procedure: For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed, if applicable anti-virus technology exists.		
5.1.1	Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?	□	□
	Test Procedure: For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).		
	All Firebox appliances provide Gateway AntiVirus (GAV) support that serve to reduce the ingress of malware into the network. While this does not address this requirement directly, using a GAV helping to meet the objectives of this requirement.		
	Firebox appliance Logs are updated whenever traffic is denied by the GAV and whenever the signature sets are updated.		
5.2	Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?	□	□
	Test Procedure: Verify that all anti-virus software is current, actively running, and capable of generating logs by performing the following: a. Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions. b. Verify that the master installation of the software is enabled for automatic updates and periodic scans. c. For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled. d. For a sample of system components, verify that antivirus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7		
	If the Firebox GAV is chosen to help with this requirement, all Fireboxes provide automatic updates of the GAV signature database, helping to meet the objectives of this requirement.		
	Firebox appliance Logs are updated whenever traffic is denied by the GAV and whenever the signature sets are updated.		

Maintain a Vulnerability Management Program *Requirement 6: Develop and maintain secure systems and applications*			
	Question	**Yes**	**No**
	In addition to the WatchGuard capabilities, additional reviews should be performed on development and maintenance to ensure secure systems and applications outside of the WatchGuard capabilities.		
6.1.a	Do all systems components and software have the latest vendor-supplied security patches installed?	□	□
	Test Procedure: For a sample of system components 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.		
	WatchGuard LiveSecurity® Service gives you access to updates and enhancements for Firebox products, including minor software patches and new software versions.		
6.1.b	Are critical security patches installed within one month of release? *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (e.g., public-facing devices and systems, databases) higher than less-critical internal devices to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	□	□
	Test Procedure: Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.		
	WatchGuard LiveSecurity® Service gives you access to updates and enhancements for Firebox products, including minor software patches and new software versions.		
6.2.a	Is there a process to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet)?	□	□
	Test Procedure: Interview responsible personnel to verify that processes are implemented to identify new security vulnerabilities.		
	WatchGuard LiveSecurity Service Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats, then delivers LiveSecurity Service alerts that describe what can be done to address each new menace.		
6.2.b	Are configuration standards updated as required by PCI DSS Requirement 2.2 to address new vulnerability issues?	□	□
	Test Procedure: Verify that processes to identify new security vulnerabilities include using outside sources for security vulnerability information and updating the system configuration standards reviewed in Requirement 2.2 as new vulnerability issues are found.		
	WatchGuard LiveSecurity Service Rapid Response Team, a dedicated group of network security experts, monitors the Internet to identify emerging threats, then delivers LiveSecurity Service alerts that describe what can be done to address each new menace.		
6.3.a	Are software applications developed in accordance with PCI DSS (e.g., secure authentication and logging) and based on industry best practices, and do they incorporate information security throughout the software development life cycle?	□	□
	Test Procedure: a. Obtain and examine written software development processes to verify that the processes are based on industry standards, security is included throughout the life cycle, and software applications are developed in accordance with PCI DSS. b. 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 the following control test procedures.		
6.3.b	Do controls ensure the following:		
6.3.1	Testing of all security patches and system and software configuration changes before deployment, including but not limited to the following?	□	□

Maintain a Vulnerability Management Program *Requirement 6: Develop and maintain secure systems and applications*			
	Question	**Yes**	**No**
	Test Procedure: Verify that all changes (including patches are tested before being deployed into production.		
6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)?	□	□
	Test Procedure: Validate all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)		
6.3.1.2	Validation of proper error handling?	□	□
	Test Procedure: Validate proper error handling.		
6.3.1.3	Validation of secure cryptographic storage?	□	□
	Test Procedure: Validate secure cryptographic storage.		
6.3.1.4	Validation of secure communications?	□	□
	Test Procedure: Validate secure communications.		
6.3.1.5	Validation of proper role-based access control (RBAC)?	□	□
	Test Procedure: Validate proper role-based access control (RBAC).		
6.3.2	Do controls ensure separate development, test, and production environments?	□	□
	Test Procedure: Verify that development and test environments are separated from the production environment, with access control in place to enforce this separation.		
6.3.3	Do controls ensure separation of duties between development, test, and production environments?	□	□
	Test Procedure: Verify that there is a separation of duties between personnel assigned to the development and test environments and those assigned to the production environment.		
6.3.4	Production data (live PANs) are not used for testing or development?	□	□
	Test Procedure: Verify that 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?	□	□
	Test Procedure: Verify that test data and accounts are removed before a production system becomes active.		
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers?	□	□
	Test Procedure: Verify that custom application accounts, user IDs and passwords are removed before a 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? *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. Code reviews can be conducted by knowledgeable internal personnel. Web applications are also subject to additional controls, if they are public-facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	□	□

Maintain a Vulnerability Management Program *Requirement 6: Develop and maintain secure systems and applications*			
	Question	**Yes**	**No**
	Test Procedure: a. Obtain and review policies to confirm that all custom application code changes for internal applications must be reviewed (either manually or with automated processes), as follows: – Code changes are reviewed by individuals other then the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. – Appropriate corrections are implemented prior to release. – Code Review results are reviewed and approved by management prior to release. b. Obtain and review policies to confirm that all custom application code changes for web applications must be reviewed (either manually or with automated processes), as follows: – Code changes are reviewed by individuals other then the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. – Code reviews ensure code is developed according to secure coding guidelines such as the Open Web Security Project Guide (see PCI DSS Requirement 6.5). – Appropriate corrections are implemented prior to release. – Code Review results are reviewed and approved by management prior to release. c. Select a sample of recent custom application changes and verify that custom application code is reviewed according to testing procedures a and b above.		
6.4.a	Are change control procedures followed for all changes to system components?	□	□
	Test Procedure: a. Obtain and examine company change control procedures related to implementing security patches and software modifications. Verify that the procedures require items 6.4.1 through 6.4.4 below. b. For a sample of system components and recent changes and security patches, trace those changes back to related change control documentation. For each change that is examined, perform the following test procedures.		
6.4.b	Do controls ensure the following:		
6.4.1	Documentation of impact?	□	□
	Test Procedure: 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?	□	□
	Test Procedure: Verify that management sign-off by appropriate parties is present for each sampled change.		
6.4.3	Testing of operational functionality?	□	□
	Test Procedure: Verify that operational functionality testing is performed for each sampled change.		
6.4.4	Back-out procedures?	□	□
	Test Procedure: Verify that back-out procedures are prepared for each sampled change.		
6.5.a	Are all web applications (internal and external, and including web administrative access to application) developed based on secure coding guidelines such as the Open Web Application Security Project guidelines?	□	□
	Test Procedure: 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 guide (http://www.owasp.org). b. Interview a sample of developers and obtain evidence that they are knowledgeable of secure coding techniques. c. Verify that processes are in place to ensure that web applications are not vulnerable to the vulnerabilities:		
6.5.b	Is prevention of common coding vulnerabilities covered in software development processes to include the following:		
6.5.1	Cross-site scripting (XSS)?	□	□

Maintain a Vulnerability Management Program *Requirement 6: Develop and maintain secure systems and applications*			
	Question	**Yes**	**No**
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to cross-site scripting (XSS). (Validate all parameters before inclusion.)		
6.5.2	Injection flaws, particularly structured query language (SQL) injection? *Also consider LDAP and Xpath injection flaws as well as other injection flaws.*	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to injection flaws, particularly structured query language (SQL) injection. (Validate input to verify user data cannot modify the meaning of commands and queries.)		
6.5.3	Malicious file execution?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to malicious file execution. (Validate input to verify application does not accept filenames or files from users.)		
6.5.4	Insecure direct object references?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to insecure direct object references. (Do not expose internal object references to users.)		
6.5.5	Cross-site request forgery (CSRF)?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)		
6.5.6	Information leakage and improper error handling?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to information leakage and improper error handling. (Do not leak information via error messages or other means.)		
6.5.7	Broken authentication and session management?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to broken authentication and session management. (Properly authenticate users and protect account credentials and session tokens.)		
6.5.8	Insecure cryptographic storage?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to insecure cryptographic storage. (Prevent cryptographic flaws.)		
6.5.9	Insecure communications?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to insecure communications. (Properly encrypt all authenticated and sensitive communications.)		
6.5.10	Failure to restrict URL access?	□	□
	Test Procedure: Verify that processes are in place to ensure that web applications are not vulnerable to the failure to restrict URL access. (Consistently enforce access control in presentation layer and business logic for all URLs.)		
6.6	For public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis, and are these applications protected against known attacks by applying either of the following methods? – Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or. – Installing a web-application layer firewall in front of public-facing web applications.	□	□

Maintain a Vulnerability Management Program *Requirement 6: Develop and maintain secure systems and applications*			
	Question	**Yes**	**No**
	Test Procedure: For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows: a. Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows: – At least annually – After any changes – By an organization that specializes in application security – That all vulnerabilities are corrected – That the application is re-evaluated after the corrections b. Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks. *Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.*		
	This requirement specifically addresses the potential vulnerabilities in applications accessible from the Internet and it refers specifically to the use of web application firewalls to provide a robust mechanism to mitigate application vulnerabilities (e.g. SQL injection, cross site scripting). In combination with a web application firewall, Fireboxes provide an additional layer of protection. The HTTP proxy is a high performance content filter that examines web traffic to identify suspicious content which can be a virus, spyware, or other type of intrusion. It can also protect your web server from attacks from the external network.		

Implement Strong Access Control Measures *Requirement 7: Restrict access to cardholder data by business need to know*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on access control measures outside of the WatchGuard capabilities.			
7.1.a	Is access to system components and cardholder data limited to only those individuals whose job requires such access?	□	□
	<u>Test Procedure:</u> Obtain and examine written policy for data control, and verify that the policy incorporates the following controls.		
7.1.b	Do access limitations include the following:		
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities?	□	□
	<u>Test Procedure:</u> Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.		
7.1.2	Assignment of privileges based on individual personnel’s job classification and function?	□	□
	<u>Test Procedure:</u> Confirm that privileges are assigned to individuals based on job classifications and function (also called “role-based access control” or RBAC).		
7.1.3	Requirement for an authorization form signed by management that specifies required privileges?	□	□
	<u>Test Procedure:</u> Confirm that an authorization form is required for all access, that it must specify required privileges, and that it must be signed by management.		
7.1.4	Implementation of an automated access control system?	□	□
	<u>Test Procedure:</u> Confirm that access controls are implemented via an automated access control system.		
7.2.a	Is an access control system in place for systems with multiple users to restrict access based on a user’s need to know, and is set to “deny all” unless specifically allowed?	□	□
	<u>Test Procedure:</u> Examine system settings and vendor documentation to verify that an access control system is implemented as follows.		
7.2.b	Does this access control system include the following:		
7.2.1	Coverage of all system components?	□	□
	<u>Test Procedure:</u> Confirm that access control systems are in place on all system components.		
7.2.2	Assignment of privileges to individuals based on job classification and function?	□	□
	<u>Test Procedure:</u> Confirm that access controls systems are configured to enforce privileges assigned to individuals based on job classifications and function.		
7.2.3	Default “deny-all” setting?	□	□
	<u>Test Procedure:</u> Confirm that the access control systems have a default “deny-all” setting. *Note: Some access control systems are set by default to “allow-all,” thereby permitting access unless or until a rule is written to specifically deny it.*		

Implement Strong Access Control Measures *Requirement 8: Assign a unique ID to each person with computer access*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, additional reviews should be performed on access control measures outside of the WatchGuard capabilities.			
8.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?	□	□
	Test Procedure: Verify that all users are assigned a unique ID for access to system components or cardholder data.		
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? (i.e., password, two-factor authentication (e.g., token devices, smart cards, biometrics, or public key.)	🟩 □	□
	Test Procedure: To verify that users are authenticated using unique ID and additional authentication (e.g., a password) for access to the cardholder data environment, perform the following: a. Obtain and examine documentation describing the authentication method(s) used. b. 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).		
	Firebox appliances must be configured to require authorization before allowing access to the cardholder data environment. This authentication is supported via standard authentication servers such as Active Directory and can also include two-factor authentication.		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
8.3	Is two-factor authentication incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties? *(Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACAS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.)*	🟩 □	□
	Test Procedure: To verify that two-factor authentication is implemented for all remote network access, observe an employee (e.g., an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (e.g. smart card, token, PIN) are required.		
	Firebox appliances support two-factor authentication, including RADIUS, SecureID, and individual VPN certificates.		
	Firebox appliance Logs are updated for each user authorization attempt via two-factor authentication, showing both successful and failed authorizations.		
8.4	Are all passwords rendered unreadable during transmission and storage on all system components using strong cryptography?	🟩 □	□
	Test Procedure: a. For a sample of system components, examine password files to verify that passwords are unreadable during transmission and storage. b. For service providers only, observe password files to verify that customer passwords are encrypted.		
	All management communications with Firebox appliances are done via a secure encryption-based protocol and Firebox appliances store and transmit their password information in an encrypted format.		
8.5	Are proper user authentication and password management controls in place for non-consumer users and administrators on all system components, as follows:		
8.5.1	Are addition, deletion, and modification of user IDs, credentials, and other identifier objects controlled?	□	□

Implement Strong Access Control Measures *Requirement 8: Assign a unique ID to each person with computer access*			
	Question	**Yes**	**No**
	Test Procedure: 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: a. Obtain and examine an authorization form for each ID. b. 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 from to the system.		
8.5.2	Is user identity verified before performing password resets?	□	□
	Test Procedure: Examine password procedures and observe security personnel to verify that, if a user requests a password reset by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the password is reset.		
8.5.3	Are first-time passwords set to a unique value for each user and must each user change their password immediately after the first use?	□	□
	Test Procedure: 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	Is access for any terminated user immediately revoked?	□	□
	Test Procedure: Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.		
8.5.5	Are inactive user accounts removed or disabled at least every 90 days?	□	□
	Test Procedure: Verify that inactive accounts over 90 days old are either removed or disabled.		
8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?	□	□
	Test Procedure: Verify that any accounts used by vendors to support and maintain system components are disabled, enabled only when needed by the vendor, and monitored while being used.		
8.5.7	Are password procedures and policies communicated to all users who have access to cardholder data?	□	□
	Test Procedure: Interview the users from a sample of user IDs to verify that they are familiar with password procedures and policies.		
8.5.8	Are group, shared, or generic accounts and passwords prohibited?	□	□
	Test Procedure: For a sample of system components, examine user ID lists to verify the following: a. Generic user IDs and accounts are disabled or removed. b. Shared user IDs for system administration activities and other critical functions do not exist. c. Shared and generic user IDs are not used to administer any system components.		
8.5.9	Must user passwords be changed at least every 90 days?	□	□
	Test Procedure: a. For a sample of system components, 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. b. For service providers only: review internal processes and customer user documentation to verify that customer passwords are required to be change periodically and that customers are given guidance as to when, and under what circumstances, passwords must change.		
8.5.10	Is a minimum password length of at least seven characters required?	□	□

Implement Strong Access Control Measures *Requirement 8: Assign a unique ID to each person with computer access*			
	Question	**Yes**	**No**
	<u>Test Procedure:</u> a. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at lest seven characters long. b. 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	Must passwords contain both numeric and alphabetic characters?	□	□
	<u>Test Procedure:</u> a. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to contain both numeric and alphabetic characters. b. For service providers only: review internal processes and customer user documentation to verify that customer passwords are required to obtain both numeric and alphabetic characters.		
8.5.12	Must an individual submit a new password that is different from any of the last four passwords he or she has used?	□	□
	<u>Test Procedure:</u> a. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as any of the last four passwords he or she has used. b. For service providers only: review internal processes and customer user documentation to verify that new customer passwords cannot be the same as any of the last four passwords he or she has used.		
8.5.13	Are repeated access attempts limited by locking out the user ID after no more than six attempts?	□	□
	<u>Test Procedure:</u> a. For a sample of system components, 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. b. 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	Is the lockout duration set to a minimum of 30 minutes or until administrator enables the user ID?	□	□
	<u>Test Procedure:</u> For a sample of system components, 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 a minimum of 30 minutes or until a system administrator resets the account.		
8.5.15	If a session has been idle for more than 15 minutes, must the user re-enter the password to re-activate the terminal?	□	□
	<u>Test Procedure</u>: To verify that two-factor authentication is implemented for all remote network access, observe an employee (e.g., an administrator) connecting remotely to the network and verify that both a password and an additional authentication item (e.g. smart card, token, PIN) are required.		
	Firebox appliances can be configured to set a maximum length of time the user can stay authenticated when idle to 15 minutes. After this, the user is required to re-authenticate before they are able to communicate with the cardholder data environment.		
8.5.16	Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)	□	□

Implement Strong Access Control Measures *Requirement 8: Assign a unique ID to each person with computer access*			
	Question	**Yes**	**No**
	Test Procedure: a. Review database and application configuration settings and verify that user authentication and access to databases includes the following: – All users are authenticated prior to access. – All user access to, user queries of, and user actions on (e.g., move, copy, delete), the dataset are through programmatic methods only (e.g., through stored procedures). – Direct access or queries to databases are restricted to database administrators. b. Review database applications and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).		

Implement Strong Access Control Measures

Requirement 9: Restrict physical access to cardholder data

	Question	Yes	No
	In addition to the WatchGaurd capabilities, additional reviews should be performed on physical access to cardholder data.		
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?	□	□
	<u>Test Procedure:</u> a. Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. b. Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. c. Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use		
9.1.1a	Do video cameras or other access-control mechanisms monitor individual physical access to sensitive areas? *Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only POS terminals are present such as the cashier areas in a retail store.*	□	□
	<u>Test Procedure:</u> a. Verify that video cameras or other access control mechanisms are in place to monitor the entry and exit points to sensitive areas. b. Video cameras or other mechanisms should be protected from tampering or disabling.		
9.1.1b	Is data collected from video cameras reviewed and correlated with other entities?	□	□
	<u>Test Procedure:</u> Verify that video cameras or other mechanisms are monitored.		
9.1.1c	Is data from video cameras stored for at least three months, unless otherwise restricted by law?	□	□
	<u>Test Procedure:</u> Verify that data from cameras or other mechanisms are stored for at least three months.		
9.1.2	Is physical access to publicly accessible network jacks restricted?	□	□
	<u>Test Procedure:</u> 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	Is physical access to wireless access points, gateways, and handheld devices restricted?	□	□
	<u>Test Procedure:</u> Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted.		
9.2	Are procedures in place 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 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.*	□	□
	<u>Test Procedure:</u> a. Review processes and procedures for assigning badges to employees, and visitors, and verify that these processes include the following: – Granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges. – Limited access to badge system. b. Observe people within the facility to verify that it is easy to distinguish between employees and visitors.		

Implement Strong Access Control Measures *Requirement 9: Restrict physical access to cardholder data*			
	Question	**Yes**	**No**
9.3	Are all visitors handled as follows:		
9.3.1	Authorized before entering areas where cardholder data is processed or maintained?	□	□
	Test Procedure: Observe visitors to verify the user 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 (e.g., a badge or access device) that expires and identifies the visitors as non-employees?	□	□
	Test Procedure: Examine employee and visitor badges to verify that ID badges clearly distinguish employees from visitors and 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?	□	□
	Test Procedure: Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.		
9.4.a	Is a visitor log in use to maintain a physical audit trail of visitor activity?	□	□
	Test Procedure: 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	Are visitor's name, the firm represented, and the employee authorizing physical access documented in the log?	□	□
	Test Procedure: 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.		
9.4.3	Is visitor log retained for a minimum of three months, unless otherwise restricted by law?	□	□
	Test Procedure: Verify that the visitor log is retained for at least three months.		
9.5.a	Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or back-up site, or a commercial storage facility?	□	□
	Test Procedure: Verify that media back-ups are stored in a secure location.		
9.5.b	Is this location's security reviewed at least annually?	□	□
	Test Procedure: Verify that the storage location is reviewed at least annually.		
9.6	Are all paper and electronic media that contain cardholder data physically secure?	□	□
	Test Procedure: Verify that procedures for protecting cardholder data include controls for physically securing paper and electronic media (including computers, removable electronic media, networking, and communications hardware, telecommunication lines, paper receipts, paper reports, and taxes.)		
9.7.a	Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?	□	□
	Test Procedure: Verify that a policy exists to control distribution of media containing cardholder data, and that the policy covers all distributed media including that distributed to individuals.		
9.7.b	Do controls include the following:		
9.7.1	Is the media classified so that it can be identified as confidential?	□	□
	Test Procedure: Verify that all media is classified so that it can be identified as "confidential."		

Implement Strong Access Control Measures
Requirement 9: Restrict physical access to cardholder data

	Question	Yes	No
9.7.2	Is the media sent by secure courier or other delivery method that can be accurately tracked?	□	□
	<u>Test Procedure:</u> Verify that all media sent outside the facility is logged and authorized by management and sent via secured courier or other delivery method that can be tracked.		
9.8	Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)?	□	□
	<u>Test Procedure:</u> Select a recent sample of several days of offsite tracking logs for all media containing cardholder data, and verify the presence in the logs of tracking details and proper management authorization.		
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?	□	□
	<u>Test Procedure:</u> 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.a	Are inventory logs of all media properly maintained?	□	□
	<u>Test Procedure:</u> Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.		
9.9.1.b	Are media inventories conducted at least annually?	□	□
	<u>Test Procedure:</u> Obtain and review the media inventory log to verify that periodic media inventories are performed at least annually.		
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons?	□	□
	<u>Test Procedure:</u> Obtain and examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following :		
	Destruction should be as follows:		
9.10.1	Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	□	□
	<u>Test Procedure:</u> a. Verify that hard-copy materials are cross-cut shredded, incinerated, or pulped such that there is reasonable assurance that hard copy materials cannot be reconstructed. 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 to its contents.		
9.10.2	Is electronic media with cardholder data rendered unrecoverable so that cardholder data cannot be reconstructed?	□	□
	<u>Test Procedure:</u> Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (e.g., degaussing).		

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data

	Question	Yes	No
	In addition to the WatchGuard capabilities, penetration tests and additional security testing reviews should be performed on systems and processes outside of the WatchGuard capabilities. Penetration tests should be performed by approved PCI vendors only.		
10.1	Is a process in place to link all access to system components (especially access done with administrative privileges such as root) to each individual user?	[✓ □]	□
	<ins>Test Procedure</ins>: Verify that audit trails are enabled and active for system components.		
	Pertains to being able to trace each login activity to an individual. Per Firebox configuration to satisfy Requirement 8.2, it is best to use an Active Directory type solution for tracking identity and logging access. All Firebox appliances support authentication via Active Directory		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:		
10.2.1	All individual accesses to cardholder data?	[✓ □]	□
	<ins>Test Procedure</ins>: Through interviews, examination of audit logs, and examination of audit log settings – verify all individual access to cardholder data is logged.		
	In order to access cardholder data, users must first authenticate to the Firebox.		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
10.2.2	All actions taken by any individual with root or administrative privileges?	[✓ □]	□
	<ins>Test Procedure</ins>: Through interviews, examination of audit logs, and examination of audit log settings – verify actions taken by any individual with root or administrative privileges is logged.		
	In order to access cardholder data, users must first authenticate to the Firebox.		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations. All Administrator accesses to the Firebox are also logged.		
10.2.3	Access to all audit trails?	□	□
	<ins>Test Procedure:</ins> Through interviews, examination of audit logs, and examination of audit log settings – verify access to all audit trails.		
10.2.4	Invalid logical access attempts?	[✓ □]	□
	<ins>Test Procedure</ins>: Through interviews, examination of audit logs, and examination of audit log settings – verify invalid logical access attempts are logged.		
	In order to access cardholder data, users must first authenticate to the Firebox.		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
10.2.5	Use of identification and authentication mechanisms?	[✓ □]	□
	<ins>Test Procedure</ins>: Through interviews, examination of audit logs, and examination of audit log settings – verify use of identification and authentication mechanisms is logged.		
	In order to access cardholder data, users must first authenticate to the Firebox.		
	Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
10.2.6	Initialization of the audit logs?	[✓ □]	□
	<ins>Test Procedure</ins>: Through interviews, examination of audit logs, and examination of audit log settings – verify initialization of audit logs is logged.		

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data

	Question	Yes	No
	Firebox appliance Logs are updated with a message indicating the start of logging upon appliance initialization.		
10.2.7	Creation and deletion of system-level objects?	□	□
	Test Procedure: Through interviews, examination of audit logs, and examination of audit log settings – verify creation and deletion of system-level objects.		
10.3	Are the following audit trail entries recorded for all system components for each event:		
10.3.1	User identification?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that user identification is included in log entries.		
	For a firewall deployment, this requirement pertains to ensuring that any configuration changes to the network components used to access and/or isolate the stored data are logged. All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated. Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
10.3.2	Type of event?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that type of event is included in log entries.		
	All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated, and whether the authorization succeeded or failed. These events are explicitly identified as authorization events in the Firebox appliance logs.		
10.3.3	Date and time?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that date and time stamp are included in log entries.		
	All Firebox appliances log entries include a date and time stamp.		
10.3.4	Success or failure indication?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that success or failure indication is included in log entries.		
	All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated, and whether the authorization succeeded or failed. These events are explicitly identified as authorization events in the Firebox appliance logs.		
10.3.5	Origination of event?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that origination of event is included in log entries.		
	All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated, and whether the authorization succeeded or failed. These events are explicitly identified as authorization events in the Firebox appliance logs.		
10.3.6	Identity or name of affected data, system component, or resource?	[✓ □]	□
	Test Procedure: For each auditable event (i.e., from 10.2) – verify that identity or name of affected data, system component, or resources is included in log entries.		
	All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated, and whether the authorization succeeded or failed. These events are explicitly identified as authorization events in the Firebox appliance logs.		
10.4	Are all critical system clocks and times synchronized?	[✓ □]	□

Regularly Monitor and Test Networks *Requirement 10: Track and monitor all access to network resources and cardholder data*			
	Question	**Yes**	**No**
	<u>Test Procedure</u>: 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. Verify the following is included in the process and implemented: a. Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2, is used for time synchronization. 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.] c. Verify that specific external hosts are designated from which the timeservers will accept NTP time updates (to prevent a malicious individual 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		
	All Fireboxes support NTP synchronization.		
10.5.a	Are audit trails secured so they cannot be altered?	[✓ □]	□
	<u>Test Procedure</u>: Interview system administrator and examine permissions to verify that audit trails are secured.		
	This can be achieved in by either configuring the Firebox to send log data to a SIEM via SNMP, or by using the Firebox proprietary logging. If the Firebox logs are used, then the Log server must be on a secure machine, and all interactions with the Firebox are secure. Firebox appliances also support sending log data to syslog servers, but this is not recommended as this is not a secure solution.		
10.5.b	Do controls ensure the following:		
10.5.1	Is viewing of audits trails limited to those with a job-related need?	□	□
	<u>Test Procedure:</u> Interview system administrator and examine permissions to verify that viewing of audit trails is limited to those with a job-related need.		
10.5.2	Are audit trail files protected from unauthorized modifications?	□	□
	<u>Test Procedure:</u> Interview system administrator and examine permissions to verify that audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and network segregation.		
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?	□	□
	<u>Test Procedure:</u> Interview system administrator and examine permissions to verify that audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.		
10.5.4	Are logs for external-facing technologies written onto a log server on the internal LAN?	[✓ □]	□
	<u>Test Procedure</u>: Verify that logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media.		
	If Firebox X Edge wireless access points are used, this is achievable by using WatchGuard Log server.		
10.5.5	Is file integrity monitoring and change detection software used on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)?	□	□
	<u>Test Procedure:</u> 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.		

Regularly Monitor and Test Networks *Requirement 10: Track and monitor all access to network resources and cardholder data*			
	Question	**Yes**	**No**
10.6	Are logs for all system components reviewed at least daily? (*Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).*) *Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.)*	□	□
	<u>Test Procedure</u>: 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. b. Through observation and interviews, verify that regular log reviews are performed for all system components.		
	WatchGuard Log Viewer can be used to search Firebox appliance logs sent to the WatchGuard Log server for specific event types.		
10.7	Is audit trail history retained for at least one year, with a minimum of three months history immediately available for analysis (for example: online, archived, or restorable from back-up.)?	□	□
	<u>Test Procedure:</u> 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. b. Verify that audit logs are available for at least one year and processes are in place to restore at least the last three months' logs for immediate analysis.		

Regularly Monitor and Test Networks *Requirement 11: Regularly test security systems and processes*			
	Question	**Yes**	**No**
In addition to the WatchGuard capabilities, penetration tests and additional security testing reviews should be performed on systems and processes outside of the WatchGuard capabilities. Penetration tests should be performed by approved PCI vendors only.			
11.1	Is the presence of wireless access points tested for by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use?	□	□
	<u>Test Procedure:</u> a. Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices. b. If a wireless IDS/IPS is implemented, verify the configuration will generate alerts to personnel. c. Verify the organization's Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.		
11.2	Are internal and external network vulnerability scans run 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)? Note: *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by the Payment Card Industry Standards Council. Scans conducted after network changes may be performed by the company's internal staff.*	□	□
	<u>Test Procedure:</u> a. Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes rescans until passing results are obtained. *Note: External scans conducted after network changes and internal scans, may be performed by the company's qualified internal personnel or third parties.* b. Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that: – Four quarterly scans occurred in the most recent 12-months period; – The results of each scan satisfy the PCI Security Scanning Procedures (e.g., no urgent, critical, or high vulnerabilities); – The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. *Note: It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance if the assessor verifies (1) the most recent scan result was a passing scan, (2) the entity has documented policies and procedures requiring quarterly scanning, and (3) vulnerabilities noted in the scan results have been corrected as show in a re-scan. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.* c. Verify that internal and external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes rescans until passing results are obtained.		
11.3	Is external and internal penetration testing performed 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)?	□	□

Regularly Monitor and Test Networks
Requirement 11: Regularly test security systems and processes

	Question	Yes	No
	Test Procedure: a. 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 noted vulnerabilities were corrected and testing repeated. b. Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).		
11.3.1	Do these penetration tests include network-layer penetration tests?	□	□
	Test Procedure: Verify that the penetration test includes network-layer penetration tests. These tests should include components that support network functions as well as operation systems.		
11.3.2	Do these penetration tests include application-layer penetration tests?	□	□
	Test Procedure: Verify that the penetration test includes application-layer penetration tests. For web applications, the tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5.		
11.4.a	Are intrusion-detection systems or intrusion-prevention systems used to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises?	□	□
	Test Procedure: a. Verify the use of intrusion-detection systems and/or intrusion-prevention systems and that all traffic in the cardholder data environment is monitored. b. Confirm IDS and/or IPS are configured to alert personnel of suspected compromises.		
	While not addressing the needs of this requirement for the whole network, the Firebox Intrusion Prevention Service (IPS) security subscription can be used to help address this requirement. While it is not recommended that the Firebox IPS solution be the only IPS system deployed in the network, use of the Firebox IPS is a great complement to addressing this requirement.		
11.4.b	Are all intrusion detection and prevention engines kept up-to-date?	□	□
	Test Procedure: Examine IDS/IPS configurations and confirm IDS/IPS devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.		
	While not addressing the needs of this requirement for the whole network, the Firebox Intrusion Prevention Service (IPS) security subscription can be used to help address this requirement. While it is not recommended that the Firebox IPS solution be the only IPS system deployed in the network, use of the Firebox IPS is a great complement to addressing this requirement.		
11.5	Is file integrity monitoring software deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and is the software configured to perform critical file comparisons at least weekly? *Note: 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 customer applications, must be evaluated and defined by the entity (that is the merchant or service provider).*	□	□
	Test Procedure: 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. Examples of files that should be monitored: a. System executables b. Application executables c. Configuration and parameter files d. Centrally stored, historical or archived, log and audit files		

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for employees and contractors

	Question	Yes	No
	In addition to the WatchGuard capabilities additional reviews should be performed to ensure adequate information security policies and training are maintained.		
12.1	Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:	□	□
	Test Procedure: 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	Do you have a security policy that addresses all of the PCI DSS requirements?	□	□
	Test Procedure: Verify that the policy addresses all PCI DSS requirements.		
12.1.2	Do you have a security policy that includes an annual process to identify threats and vulnerabilities, and which results in a formal risk assessment?	□	□
	Test Procedure: Verify that the information security policy includes an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.		
	Fireboxes enable continuous risk management, proactively identifying and mitigating unauthorized network activity that may jeopardize the integrity and security of the cardholder data environment and the IT infrastructure. Unauthorized network activity is logged in multiple ways in the appliance logs, including: • User authorization successes and failures • Unauthorized traffic denied entry to the cardholder data environment • Intrusion protection events • AntiVirus scanning results		
12.1.3	Do you have a security policy that includes a review at least once a year and updates when the environment changes?	□	□
	Test Procedure: 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	Are daily operational security procedures developed that are consistent with requirements in this specification (e.g., user account maintenance procedures, and log review procedures)?	□	□
	Test Procedure: 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.a	Are usage policies for critical employee-facing technologies (e.g., remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email and Internet usage) developed to define proper use of these technologies for all employees and contractors?	□	□
	Test Procedure: Obtain and examine the policy for critical employee-facing technologies and perform the steps listed below in 12.3.1 through 12.3.10.		
	WatchGuard provides active security policy enforcement and authorization. Through its Virtual Private Networking technology (both IPSec and SSL) WatchGuard facilitates the elimination of unauthorized access to critical employee-facing technologies.		
	Firebox appliances log all VPN login attempts, success or failure.		
12.3.1	Do the usage policies require explicit management approval?	□	□
	Test Procedure: Verify that the usage policies require explicit management approval to use the technologies.		
12.3.2	Do the usage policies require authentication for use of the technology?	□	□
	Test Procedure: Verify that the usage policies require that all technology use be authenticated with user ID and password or other authentication item (e.g., token).		

Maintain an Information Security Policy *Requirement 12: Maintain a policy that addresses information security for employees and contractors*			
	Question	**Yes**	**No**
	Fireboxes are configured to require authorization before allowing access to the cardholder data environment providing active security policy enforcement and authentication. This authentication is supported via standard authentication servers such as Active Directory and can also include two factor authentication		
	All Firebox appliances will log user login and configuration changes, including the user name and IP address of the machine from which the login was initiated. Firebox appliance Logs are updated for each user authorization attempt, showing both successful and failed authorizations.		
12.3.3	Do the usage policies require listing of all such devices and personnel with access?	□	□
	Test Procedure: Verify that the usage policies require a list of all devices and personnel authorized to use the devices.		
12.3.4	Do the usage policies require labeling of devices with owner, contact information, and purpose?	□	□
	Test Procedure: Verify that the usage policies require labeling of devices with owner, contact information, and purpose.		
12.3.5	Do the usage policies require acceptable uses of the technologies?	□	□
	Test Procedure: Verify that the usage policies require acceptable uses for the technology.		
12.3.6	Do the usage policies require acceptable network locations for the technologies?	□	□
	Test Procedure: Verify that the usage policies require acceptable network locations for the technology.		
12.3.7	Do the usage policies require a list of company-approved products?	□	□
	Test Procedure: Verify that the usage policies require a list of company-approved products.		
12.3.8	Do the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?	□	□
	Test Procedure: Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.		
12.3.9	Do the usage policies require activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use?	□	□
	Test Procedure: Verify that the usage policies require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.		
12.3.10	When accessing cardholder data remotely via remote-access technologies, does the policy specify the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media?	□	□
	Test Procedure: Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives, and removable electronic media when accessing such data via remote-access technologies.		
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?	□	□
	Test Procedure: Verify that information security policies clearly define information security responsibilities for both employees and contractors.		
12.5	Are the following information security management responsibilities assigned to an individual or team: 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	Do you establish, document, and distribute security policies and procedures?	□	□

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for employees and contractors

	Question	**Yes**	**No**
	Test Procedure: Verify that responsibility for creating and distributing security policies and procedures is formally assigned.		
12.5.2	Do you monitor and analyze security alerts and information, and distribute to appropriate personnel?	□	□
	Test Procedure: Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.		
	WatchGuard provides real-time SNMP and email alerts when an event occurs that is a possible security threat. When violations are found, WatchGuard provides automated remediation, e.g. allow, block the ports on which a threat appeared, block the IP address that sent the packets and report the violation.		
	WatchGuard generates a report that shows automatically generated alerts.		
12.5.3	Have you established, documented, and distributed security incident response and escalation procedures to ensure effective handling of all situations?	□	□
	Test Procedure: Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.		
12.5.4	Do you administer user accounts, including additions, deletions, and modifications?	□	□
	Test Procedure: Verify that responsibility for administering user account and authentication management is formally assigned.		
12.5.5	Do you monitor and control all access to data?	□	□
	Test Procedure: Verify that responsibility for monitoring and controlling all access to data is formally assigned.		
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?	□	□
	Test Procedure: a. Verify the existence of formal security awareness program for all employees. b. Obtain and examine security awareness program procedures and documentation and perform the following:		
12.6.1	Are employees educated upon hire and at least annually (e.g., by letters, posters, memos, meetings, and promotions)?	□	□
	Test Procedure: a. Verify that the security awareness program provides multiple methods of communicating awareness and education employees (e.g., posters, letters, memos, web-based training, meetings, and promotions). b. Verify that employees attend awareness training upon hire and at least annually		
12.6.2	Are employees required to acknowledge at least annually that they have read and understood the company's security policy and procedures?	□	□
	Test Procedure: Verify that the security awareness program requires employees to acknowledge (e.g., in writing or electronically) at least annually that they have read and understand the company's information security policy.		
12.7	Are potential employees (see definition of "employee" at 9.2 above) screened 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 facilitation a transaction, this requirement is a recommendation only.*	□	□

Maintain an Information Security Policy *Requirement 12: Maintain a policy that addresses information security for employees and contractors*			
	Question	**Yes**	**No**
	Test Procedure: Inquire with Human Resources department management and verify that background checks are conducted (within the constraints of local laws) on employees prior to hire who have access to cardholder data or the cardholder data environment. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)		
12.8	If cardholder is shared with service providers, are policies and procedures maintained and implemented to manage service providers, and do the policies and procedures include the following?	□	□
	Test Procedure: If the entity being assessed shares cardholder data with service providers (e.g., back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), through observations, review of policies and procedures, and review of supporting documentation, perform the following:		
12.8.1	A list of service providers is maintained?	□	□
	Test Procedure: Verify that a list of service providers is maintained.		
12.8.2	A written agreement that includes an acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses?	□	□
	Test Procedure: Verify that the written agreement includes an acknowledgement by the service provider of their responsibility for security cardholder data.		
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement?	□	□
	Test Procedure: Verify that policies and procedures are documented and were followed including proper due diligence prior to engaging any service provider.		
12.8.4	A program is maintained to monitor service provider PCI DSS compliance status?	□	□
	Test Procedure: Verify that the entity assessed maintains a program to monitor its service providers' PCI DSS compliance status.		
12.9	Has an incident response plan been implemented to include the following in preparation to respond immediately to a system breach? Obtain and examine the Incident Response Plan and related procedures and perform the following:		
12.9.1.a	Has an incident response plan been created to be implemented in the event of system breach?	□	□
	Test Procedure: Verify that the Incident Response Plan has been created and implemented to address a system breach.		
12.9.1.b	Does the plan address, at a minimum, specific incident response procedures, business recover and continuity procedures, data backup processes, roles and responsibilities, analysis of legal requirements for reporting compromises, coverage and responses of all critical system components, reference or inclusion of incident respond procedures from the payment brands, and communication and contact strategies (e.g., informing the acquires and payment card associations)?	□	□

Maintain an Information Security Policy *Requirement 12: Maintain a policy that addresses information security for employees and contractors*			
	Question	**Yes**	**No**
	Test Procedure: Verify that the Incident Response Plan includes: a. Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. b. Specific incident response procedures. c. Business recovery and continuity procedures. d. Data back-up processes. e. Analysis of legal requirements for reporting compromises (e.g., California Bill 1386 and similar laws in most other States, which require notification of affected consumers in the event of an actual or suspected compromise for any business with that State's residents in their database.) f. Coverage and responses for all critical system components. g. Reference or inclusion of incident response procedures from the payment brands.		
12.9.2	Is the plan tested at least annually?	□	□
	Test Procedure: Verify that the plan is tested at least annually.		
12.9.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?	□	□
	Test Procedure: Verify through observation and review of policies that there is 24/7 response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and reports of unauthorized critical system or content file changes.		
12.9.4	Is appropriate training provided to staff with security breach response responsibilities?	□	□
	Test Procedure: Verify through observation and review of policies that staff with security breach responsibilities are periodically trained.		
12.9.5	Are alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems included?	□	□
	Test Procedure: Verify through observation and review of processes that monitoring and responding to alerts from security systems including detection of unauthorized wireless access points are covered in the Incident Response Plan.		
12.9.6	Is process developed and in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments?	□	□
	Test Procedure: 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.		

Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where “YES” was checked and compensating controls were mentioned.

Note: 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.

Requirement Number and Definition: ______

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement	
2. Objective	Define the objective of the original control. Identify the objective met by the compensating control.	
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	
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.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process and controls in place to maintain compensating controls.	