



Attestation of Compliance, SAQ D—Merchant Version

Instructions for Submission

The merchant must complete this Attestation of Compliance as a declaration of the merchant's compliance status with the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Security Assessment Procedures*. Complete all applicable sections and refer to the submission instructions at PCI DSS Compliance – Completion Steps in this document.

Part 1. Qualified Security Assessor Company Information (if applicable)

Company Name:					
Lead QSA Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

Part 2. Merchant Organization Information

Company Name:	Pukka Software	DBA(S):	MotorsportReg.com		
Contact Name:	Brian Ghidinelli	Title:	Owner		
Telephone:	415.462.5603	E-mail:	brian@pukkasoft.com		
Business Address:	236 N. Santa Cruz Ave #252	City:	Los Gatos		
State/Province:	CA	Country:	USA	ZIP:	95030
URL:	http://www.MotorsportReg.com				

Part 2a. Type of merchant business (check all that apply):

- Retailer Telecommunication Grocery and Supermarkets
 Petroleum E-Commerce Mail/Telephone-Order
 Others (please specify):

List facilities and locations included in PCI DSS review: Pukka Software, 236 N. Santa Cruz #252, Los Gatos, CA 95030 // Layer42 Networks, 3080 Raymond Street, Santa Clara, CA // Greensoft Solutions, Inc., 10828 AirWorld Drive, Kansas City, MO 64153

Part 2b. Relationships

Does your company have a relationship with one or more third-party service providers (for example, gateways, web-hosting companies, airline booking agents, loyalty program agents, etc)? Yes No

Does your company have a relationship with more than one acquirer? Yes No

Part 2c. Transaction Processing

Payment Application in use: Internal	Payment Application Version: 4105
--------------------------------------	-----------------------------------

Part 3. PCI DSS Validation

Based on the results noted in the SAQ D dated 5/8/2009, *MotorsportReg.com* asserts the following compliance status (check one):

- Compliant:** All sections of the PCI SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating; **and** a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby *MotorsportReg.com* has demonstrated full compliance with the PCI DSS.
- Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or not all questions are answered "yes," resulting in an overall **NON-COMPLIANT** rating, **or** a passing scan has not been completed by a PCI SSC Approved Scan Vendor, thereby (*Merchant Company Name*) has not demonstrated full compliance with the PCI DSS.

Target Date for Compliance:

An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

Part 3a. Confirmation of Compliant Status

Merchant confirms:

- PCI DSS Self-Assessment Questionnaire D, Version 1.2, was completed according to the instructions therein.
- All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
- I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
- I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
- No evidence of magnetic stripe (i.e., track) data², CAV2, CVC2, CID, or CVV2 data³, or PIN data⁴ storage after transaction authorization was found on ANY systems reviewed during this assessment.

Part 3b. Merchant Acknowledgement

	5/8/2009
<i>Signature of Merchant Executive Officer</i> ↑	<i>Date</i> ↑
Brian Ghidinelli	Owner
<i>Merchant Executive Officer Name</i> ↑	<i>Title</i> ↑
Pukka Software / MotorsportReg.com	
<i>Merchant Company Represented</i> ↑	

² Data encoded in the magnetic stripe used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization. The only elements of track data that may be retained are account number, expiration date, and name.

³ The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

⁴ Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Self-Assessment Questionnaire D

Date of Completion:

Build and Maintain a Secure Network

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

Question	Response:	Yes	No	Special*
		<input type="checkbox"/>	<input type="checkbox"/>	
1.1 Do established firewall and router configuration standards include the following?				
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall and router configurations?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.1.2 Current network diagrams with all connections to cardholder data, including any wireless networks?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.1.4 Description of groups, roles, and responsibilities for logical management of network components?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.1.6 Requirement to review firewall and router rule sets at least every six months)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.2 Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder data environment as follows: <i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>				
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
1.2.2 Secure and synchronize router configuration files?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?				
1.3.1	Is a DMZ implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder environment?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.3.2	Is inbound Internet traffic limited to IP addresses within the DMZ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.3.3	Are direct routes prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.3.4	Are internal addresses prohibited from passing from the Internet into the DMZ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.3.7	Is the database placed in an internal network zone, segregated from the DMZ?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
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? <i>Use Network address translation (NAT) technologies—for example, port address translation (PAT).</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
1.4	Has personal firewall software been installed on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network?	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

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

Question		Response: <u>Yes</u> <u>No</u>		<u>Special*</u>
2.1	Are vendor-supplied defaults always changed before installing a system on the network? <i>Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.1.1	(a) Are defaults** for wireless environments connected to the cardholder data environment or transmitting cardholder data changed before installing a wireless system? <i>** Such wireless environment defaults include but are not limited to default wireless encryption keys, passwords, and SNMP community strings.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are wireless device security settings enabled for strong encryption technology for authentication and transmissions?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2	(a) Have configuration standards been developed for all system components?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do these standards address all known security vulnerabilities and are they consistent with industry-accepted system hardening standards—for example, SysAdmin Audit Network Security (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(c) Do controls ensure the following?			
2.2.1	Is only one primary function implemented per server?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.2	Are all unnecessary and insecure services and protocols disabled (services and protocols not directly needed to perform the device's specified function)?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.3	Are system security parameters configured to prevent misuse?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.2.4	Has all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers—been removed?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2.3	Is all non-console administrative access encrypted? <i>Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.</i>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

	Question	Response: <u>Yes</u> <u>No</u>		<u>Special*</u>
2.4	If you are a shared hosting provider, are your systems configured to protect each entity's hosted environment and cardholder data? See Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers <i>for specific requirements that must be met.</i>	<input type="checkbox"/>	<input type="checkbox"/>	N/A

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Question		Response:	Yes	No	Special*
3.1	(a) 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/or regulatory purposes?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2	Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.1	<p>Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.</p> <p><i>Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:</i></p> <ul style="list-style-type: none"> ▪ The cardholder's name, ▪ Primary account number (PAN), ▪ Expiration date, and ▪ Service code <p><i>To minimize risk, store only these data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements.</i></p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.2	<p>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.</p> <p><i>Note: See PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.</i></p>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.3	<p>Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)?</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ This requirement does not apply to employees and other parties with a specific need to see the full PAN; ▪ This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts. 		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
3.4	<p>Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs,) by using any of the following approaches?</p> <ul style="list-style-type: none"> ▪ 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. <p><i>The MINIMUM account information that must be rendered unreadable is the PAN.</i></p> <p><i>If for some reason, a company is unable to render the PAN unreadable, refer to Appendix B: "Compensating Controls."</i></p> <p><i>Note: "Strong cryptography" is defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.</i></p>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.4.1	If disk encryption (rather than file- or column-level database encryption) is used:				
	(a) Is logical access managed independently of native operating system access control mechanisms (for example, by not using local user account databases)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are decryption keys independent of user accounts?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.5	Are cryptographic keys used for encryption of cardholder data protected against both disclosure and misuse?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.5.1	Is access to cryptographic keys restricted to the fewest number of custodians necessary?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.5.2	Are cryptographic keys stored securely, and in the fewest possible locations and forms?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6	(a) Are all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, fully documented and implemented?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do they include the following?				
3.6.1	Generation of strong cryptographic keys		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.2	Secure cryptographic key distribution		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.3	Secure cryptographic key storage		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.4	Periodic changing of cryptographic keys: <ul style="list-style-type: none"> ▪ As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically ▪ At least annually 		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.5	Retirement or replacement of old or suspected compromised cryptographic keys		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.6	Split knowledge and establishment of dual control of cryptographic keys		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Question		Response:	Yes	No	Special*
3.6.7	Prevention of unauthorized substitution of cryptographic keys		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3.6.8	Requirement for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Question		Response:	Yes	No	Special*
4.1	<p>Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?</p> <p><i>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).</i></p>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.1.1	<p>Are industry best practices (for example, 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?</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> ▪ <i>For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.</i> ▪ <i>For current wireless implementations, it is prohibited to use WEP after June 30, 2010.</i> 		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4.2	Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Maintain a Vulnerability Management Program

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

	Question	Response:	Yes	No	Special*
5.1	Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5.2	Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 6: Develop and maintain secure systems and applications

	Question	Response:	Yes	No	Special*
6.1	(a) Do all system components and software have the latest vendor-supplied security patches installed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are critical security patches installed within one month of release? <i>Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, 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.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.2	(a) Is there a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are configuration standards updated as required by PCI DSS Requirement 2.2 to address new vulnerability issues?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3	(a) Are software applications developed in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and do they incorporate information security throughout the software development life cycle?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(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:		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.1.1	Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
6.3.1.2	Validation of proper error handling		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.1.3	Validation of secure cryptographic storage		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.1.4	Validation of secure communications		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.1.5	Validation of proper role-based access control (RBAC)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.2	Separate development/test and production environments?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.3	Separation of duties between development/test and production environments?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.4	Production data (live PANs) are not used for testing or development?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.5	Removal of test data and accounts before production systems become active?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.6	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.3.7	Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability? <i>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.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.4	(a) Are change control procedures followed for all changes to system components?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do procedures ensure the following?				
6.4.1	Documentation of impact?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.4.2	Management sign-off by appropriate parties?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.4.3	Testing of operational functionality?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.4.4	Back-out procedures?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Question		Response:	Yes	No	Special*
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 <i>Open Web Application Security Project Guide</i> ?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Is prevention of common coding vulnerabilities covered in software development processes, including the following? <i>Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.</i>				
6.5.1	Cross-side scripting (XSS)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.2	Injection flaws, particularly SQL injection? <i>Also consider LDAP and Xpath injection flaws as well as other injection flaws.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.3	Malicious file execution?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.4	Insecure direct object references?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.5	Cross-site request forgery (CSRF)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.6	Information leakage and improper error handling?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.7	Broken authentication and session management?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.8	Insecure cryptographic storage?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.9	Insecure communications?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6.5.10	Failure to restrict URL access?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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 <i>either</i> of the following methods? <ul style="list-style-type: none"> ▪ 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. 		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Implement Strong Access Control Measures

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

Question		Response:	Yes	No	Special*
7.1	(a) Is access to system components and cardholder data limited to only those individuals whose jobs require such access?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.1.2	Assignment of privileges based on individual personnel's job classification and function?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.1.3	Requirement for an authorization form signed by management that specifies required privileges?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.1.4	Implementation of an automated access control system?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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 it set to "deny all" unless specifically allowed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Does this access control system include the following:				
7.2.1	Coverage of all system components?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.2.2	Assignment of privileges to individuals based on job classification and function?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7.2.3	Default "deny-all" setting?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

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

Question		Response:	Yes	No	Special*
8.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? <ul style="list-style-type: none"> ▪ Password or passphrase ▪ Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys) 		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
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? <i>Use technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.4	Are all passwords rendered unreadable during transmission and storage on all system components using strong cryptography (defined in <i>PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms</i>)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.2	Is user identity verified before performing password resets?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.4	Is access for any terminated users immediately revoked?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.5	Are inactive user accounts removed or disabled at least every 90 days?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.7	Are password procedures and policies communicated to all users who have access to cardholder data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.8	Are group, shared, or generic accounts and passwords prohibited?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.9	Must user passwords be changed at least every 90 days?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.10	Is a minimum password length of at least seven characters required?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.11	Must passwords contain both numeric and alphabetic characters?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.13	Are repeated access attempts limited by locking out the user ID after no more than six attempts?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
8.5.14	Is the lockout duration set to a minimum of 30 minutes or until administrator enables the user ID?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8.5.16	Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 9: Restrict physical access to cardholder data

Question		Response:	Yes	No	Special*
9.1	Are appropriate facility entry controls in place to limit and monitor physical access to systems in the cardholder data environment?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.1.1	(a) Do video cameras or other access-control mechanisms monitor individual physical access to sensitive areas? <i>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 point-of-sale terminals are present such as the cashier areas in a retail store.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Is data collected from video cameras reviewed and correlated with other entries?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(c) Is data from video cameras stored for at least three months, unless otherwise restricted by law?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.1.2	Is physical access to publicly accessible network jacks restricted?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.1.3	Is physical access to wireless access points, gateways, and handheld devices restricted?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.2	Are procedures in place to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible? <i>For purposes of this requirement, an "employee" refers to full-time and part-time employees, temporary employees and personnel, and contractors 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.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.3	Are all visitors handled as follows:				
9.3.1	Authorized before entering areas where cardholder data is processed or maintained?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
9.3.2	Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.3.3	Asked to surrender the physical token before leaving the facility or at the date of expiration?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.4	(a) Is a visitor log in use to maintain a physical audit trail of visitor activity?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are the visitor's name, the firm represented, and the employee authorizing physical access documented on the log?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(c) Is visitor log retained for a minimum of three months, unless otherwise restricted by law?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.5	(a) Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Is this location's security reviewed at least annually?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.6	Are all paper and electronic media that contain cardholder data physically secure?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls include the following:				
9.7.1	Is the media classified so it can be identified as confidential?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately tracked?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.9.1	(a) Are inventory logs of all media properly maintained?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are media inventories conducted at least annually?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.10.1	Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9.10.2	Is electronic media with cardholder data rendered unrecoverable so that cardholder data cannot be reconstructed?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Regularly Monitor and Test Networks

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

Question		Response:	Yes	No	Special*
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2	Are automated audit trails implemented for all system components to reconstruct the following events:				
10.2.1	All individual user accesses to cardholder data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.2	All actions taken by any individual with root or administrative privileges?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.3	Access to all audit trails?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.4	Invalid logical access attempts?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.5	Use of identification and authentication mechanisms?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.6	Initialization of the audit logs?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.2.7	Creation and deletion of system-level object?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3	Are the following audit trail entries recorded for all system components for each event:				
10.3.1	User identification?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.2	Type of event?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.3	Date and time?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.4	Success or failure indication?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.5	Origination of event?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.3.6	Identity or name of affected data, system component, or resource?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.4	Are all critical system clocks and times synchronized?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.5	(a) Are audit trails secured so they cannot be altered?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do controls ensure the following?				
10.5.1	Is viewing of audit trails limited to those with a job-related need?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.5.2	Are audit trail files protected from unauthorized modifications?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.5.3	Are audit trail files promptly backed up to a centralized log server or media that is difficult to alter?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
10.5.4	Are logs for external-facing technologies written onto a log server on the internal LAN?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.5.5	Is file-integrity monitoring or 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)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.6	Are logs for all system components reviewed at least daily? <i>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).</i> <i>Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10.7	Is audit trail history retained for at least one year, with a minimum of three months' history immediately available for analysis (for examples, online, archived, or restorable from backup)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Requirement 11: Regularly test security systems and processes

Question		Response:	Yes	No	Special*
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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)? <i>Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11.3	(a) 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)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do these penetration tests include the following:				
11.3.1	Network-layer penetration tests?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11.3.2	Application-layer penetration tests?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

	Question	Response:	Yes	No	Special*
11.4	(a) Are intrusion-detection systems and/or intrusion-prevention systems used to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Are all intrusion-detection and prevention engines kept up-to-date?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11.5	(a) Is file-integrity monitoring software deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Is the software configured to perform critical file comparisons at least weekly? <i>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 custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Maintain an Information Security Policy

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

Question		Response:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated, and does it accomplish the following:		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.1.1	Addresses all PCI DSS requirements?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.1.2	Includes an annual process to identify threats and vulnerabilities, and which results in a formal risk assessment?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.1.3	Includes a review at least once a year and updates when the environment changes?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.2	Are daily operational security procedures developed that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures)?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3	(a) Are usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all employees and contractors?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Do these usage policies require the following?				
12.3.1	Explicit management approval?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.2	Authentication for use of the technology?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.3	A list of all such devices and personnel with access?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.4	Labeling of devices with owner, contact information, and purpose?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.5	Acceptable uses of the technologies?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.6	Acceptable network locations for the technologies?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.7	List of company-approved products?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.3.9	Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
12.3.10	When accessing cardholder data 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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5	Are the following information security management responsibilities assigned to an individual or team?				
12.5.1	Establishing, documenting, and distributing security policies and procedures?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5.2	Monitoring and analyzing security alerts and information, and distributing to appropriate personnel?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5.4	Administering user accounts, including additions, deletions, and modifications?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.5.5	Monitoring and controlling all access to data?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.6.1	Are employees educated upon hire and at least annually?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.6.2	Are employees required to acknowledge at least annually that they have read and understood the company's security policy and procedures?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.7	Are potential employees (see definition of "employee" at 9.2 above) screened prior to hire to minimize the risk of attacks from internal sources? <i>For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.</i>		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8	If cardholder data 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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.1	A list of service providers is maintained.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.2	A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.

Question		Response:	Yes	No	Special*
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.9	Has an incident response plan been implemented to include the following in preparation to respond immediately to a system breach?				
12.9.1	(a) Has an incident response plan been created to be implemented in the event of system breach?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	(b) Does the plan address, at a minimum:				
	▪ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Specific incident response procedures		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Business recovery and continuity procedures		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Data back-up processes		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Analysis of legal requirements for reporting compromises		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Coverage and responses of all critical system components		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	▪ Reference or inclusion of incident response procedures from the payment brands		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.9.2	Is the plan tested at least annually?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.9.3	Are specific personnel designated to be available on a 24/7 basis to respond to alerts?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.9.4	Is appropriate training provided to staff with security breach response responsibilities?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12.9.5	Are alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems included?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	

* "Not Applicable" (N/A) or "Compensating Control Used." Organizations using this section must complete the Compensating Control Worksheet or Explanation of Non-Applicability Worksheet, as appropriate, in the Appendix.