Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire C
and Attestation of Compliance

Payment Application Connected to Internet,
No Electronic Cardholder Data Storage

Version 1.2

October 2008

Document Changes

Date	Version	Description
October 1, 2008	1.2	To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.

Table of Contents

PCI Data Security Standard: Related Documents

The following documents were created to assist merchants and service providers in understanding the PCI Data Security Standard and the PCI DSS SAQ.

Document	Audience
PCI Data Security Standard Requirements and Security Assessment Procedures	All merchants and service providers
Navigating PCI DSS: Understanding the Intent of the Requirements	All merchants and service providers
PCI Data Security Standard: Self-Assessment Guidelines and Instructions	All merchants and service providers
PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation	Merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation	Merchants[1] and all service providers
PCI Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms	All merchants and service providers

---

[1] To determine the appropriate Self-Assessment Questionnaire, see *PCI Data Security Standard: Self-Assessment Guidelines and Instructions*, "Selecting the SAQ and Attestation That Best Apply To Your Organization."

Before you Begin

Completing the Self-Assessment Questionnaire

SAQ C has been developed to address requirements applicable to merchants who process cardholder data via payment applications (for example, POS systems) connected to the Internet (via high-speed connection, DSL, cable modem, etc.), but who do not store cardholder data on any computer system. These payment applications are connected to the Internet either because:

1. The payment application is on a personal computer connected to the Internet, or

2. The payment application is connected to the Internet to transmit cardholder data.

These merchants are defined as SAQ Validation Type 4, as defined here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*. Validation Type 4 merchants process cardholder data via POS machines connected to the Internet, do not store cardholder data on any computer system, and may be either brick-and-mortar (card-present) or e-commerce or mail/telephone-order (card-not-present) merchants. Such merchants must validate compliance by completing SAQ C and the associated Attestation of Compliance, confirming that:

- Your company has a payment application system and an Internet connection on the same device;

- The payment application/Internet device is not connected to any other systems within your environment;

- Your company retains only paper reports or paper copies of receipts;

- Your company does not store cardholder data in electronic format; and

- Your company's payment application vendor uses secure techniques to provide remote support to your payment system.

Each section of this questionnaire focuses on a specific area of security, based on the requirements in the PCI Data Security Standard.

PCI DSS Compliance – Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ C) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines.*

2. Complete a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.

3. Complete the Attestation of Compliance in its entirety.

4. Submit the SAQ, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

Guidance for Non-Applicability and Exclusion of Certain, Specific Requirements

Exclusion: If you are required to answer SAQ C to validate your PCI DSS compliance, the following exception may be considered. See "Non-Applicability" below for the appropriate SAQ response.

- The questions specific to wireless only need to be answered if wireless is present anywhere in your network (for example, Requirement 2.1.1). Note that Requirement 11.1 (use of wireless analyzer) must still be answered even if wireless is not in your network, since the analyzer detects any rogue or unauthorized devices that may have been added without the merchant's knowledge.

Non-Applicability: This and any other requirements deemed not applicable to your environment must be indicated with "N/A" in the "Special" column of the SAQ. Accordingly, complete the "Explanation of Non-Applicability" worksheet in the Appendix for each "N/A" entry.

Attestation of Compliance, SAQ C

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:		DBA(S):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					

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:

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:	Payment Application Version:

Part 2d. Eligibility to Complete SAQ C

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

☐	Merchant has a payment application system and an Internet or public network connection on the same device;
☐	The payment application system/Internet device is not connected to any other system within the merchant environment;
☐	Merchant does not store cardholder data in electronic format;
☐	If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; **and**
☐	Merchant's payment application software vendor uses secure techniques to provide remote support to merchant's payment application system.

Part 3. PCI DSS Validation

Based on the results noted in the SAQ C dated *(completion date)*, *(Merchant Company Name)* asserts the following compliance status (check one):

☐   **Compliant:** All sections of the PCI SAQ are complete, and all questions answered "yes," resulting in an overall **COMPLIANT** rating, **and** a passing scan has been completed by a PCI SSC Approved Scan Vendor, thereby *(Merchant Company Name)* has demonstrated full compliance with the PCI DSS.

☐   **Non-Compliant:** Not all sections of the PCI SAQ are complete, or some questions are answered "no," 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 C, Version *(version of SAQ)*, 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) data[2], CAV2, CVC2, CID, or CVV2 data[3], or PIN data[4] storage after transaction authorization was found on ANY systems reviewed during this assessment.

---

[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.

Part 3b. Merchant Acknowledgement

Signature of Merchant Executive Officer ↑	*Date* ↑
Merchant Executive Officer Name ↑	*Title* ↑

Merchant Company Represented ↑

Part 4. Action Plan for Non-Compliant Status

Please select the appropriate "Compliance Status" for each requirement. If you answer "NO" to any of the requirements, you are required to provide the date Company will be compliant with the requirement and a brief description of the actions being taken to meet the requirement. *Check with your acquirer or the payment brand(s) before completing Part 4, since not all payment brands require this section.*

PCI DSS Requirement	Description of Requirement	Compliance Status (Select One)		Remediation Date and Actions (if Compliance Status is "NO")
		YES	NO	
1	Install and maintain a firewall configuration to protect cardholder data	☐	☐	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	☐	☐	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
5	Use and regularly update anti-virus software	☐	☐	
6	Develop and maintain secure systems and applications	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
8	Assign a unique ID to each person with computer access	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
11	Regularly test security systems and processes	☐	☐	
12	Maintain a policy that addresses information security	☐	☐	

Self-Assessment Questionnaire C

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*
1.2	Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder data environment as follows: *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.*		☐	☐	
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment?		☐	☐	

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

	Question	Response:	Yes	No	Special*
2.1	Are vendor-supplied defaults always changed **before** installing a system on the network? *Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.*		☐	☐	
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? * *Such wireless environment defaults include but are not limited to default wireless encryption keys, passwords, and SNMP community strings.*		☐	☐	
	(b) Are wireless device security settings enabled for strong encryption technology for authentication and transmissions?		☐	☐	
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.*		☐	☐	

---

* "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.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

		Question	Response:	Yes	No	Special*
3.2		Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)?		☐	☐	
	3.2.1	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. *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 these data elements as needed for business. NEVER store the card verification code or value or PIN verification value data elements.* *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*		☐	☐	
	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. *Note: See* PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms *for additional information.*		☐	☐	
	3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.		☐	☐	
3.3		Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed). *Notes:* ▪ *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.*		☐	☐	

---

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

	Question	Response:	Yes	No	Special*
4.1	Are strong cryptography and security protocols, such as SSLTLS or 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).* *Note: If you have wireless technology implemented in your environment, please be aware of the following:* ▪ *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.* ▪ *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*		☐	☐	
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)?		☐	☐	

---

* "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?	☐	☐	
	5.1.1	Are all anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software?	☐	☐	
5.2		Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?	☐	☐	

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?	☐	☐	
	(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 (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.			

---

* "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?		☐	☐	

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

	Question	Response:	Yes	No	Special*
8.5.6	Are accounts used by vendors for remote maintenance enabled only during the time period needed?		☐	☐	

Requirement 9: Restrict physical access to cardholder data

	Question	Response:	Yes	No	Special*
9.6	Are all paper and electronic media that contain cardholder data physically secure?		☐	☐	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?		☐	☐	
	(b) Do controls include the following:				
9.7.1	Is the media classified so it can be identified as confidential?		☐	☐	
9.7.2	Is the media sent by secured courier or other delivery method that can be accurately 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)?		☐	☐	
9.9	Is strict control maintained over the storage and accessibility of media that contains cardholder data?		☐	☐	
9.10	Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons? Destruction should be as follows:		☐	☐	
9.10.1	Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		☐	☐	

---

* "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.

Regularly Monitor and Test Networks

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

Question	Response:	Yes	No	Special*
No questions applicable to SAQ C.				

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?		☐	☐	
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 Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.				

---

* "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 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:	☐	☐	
12.1.3	Includes a review at least once a year and updates when the environment changes?	☐	☐	
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?	☐	☐	
12.4	Do the security policy and procedures clearly define information security responsibilities for all employees and contractors?	☐	☐	
12.5	Are the following information security management responsibilities assigned to an individual or team?			
12.5.3	Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations?	☐	☐	
12.6	Is a formal security awareness program in place to make all employees aware of the importance of cardholder data security?	☐	☐	
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?	☐	☐	
12.8.1	A list of service providers is maintained.	☐	☐	
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 possesses	☐	☐	
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.	☐	☐	
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.	☐	☐	

---

* "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.

Appendix A: (not used)

This page intentionally left blank

Appendix B: Compensating Controls

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

1. Meet the intent and rigor of the original PCI DSS requirement.

2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See *Navigating PCI DSS* for the intent of each PCI DSS requirement.)

3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)

    When evaluating "above and beyond" for compensating controls, consider the following:

    Note: The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.

    a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords).

    b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. For example, two-factor authentication is a PCI DSS requirement for remote access. Two-factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Two-factor authentication may be an acceptable compensating control if; (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.

    c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) two-factor authentication from within the internal network.

4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.

Appendix C: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

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.	

Compensating Controls Worksheet—Completed Example

Use this worksheet to define compensating controls for any requirement where "YES" was checked and compensating controls were mentioned in the "Special" column.

Requirement Number: *8.1—Are all users identified with a unique user name before allowing them to access system components or cardholder data?*

	Information Required	Explanation
1. Constraints	List constraints precluding compliance with the original requirement.	*Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a "root" login. It is not possible for Company XYZ to manage the "root" login nor is it feasible to log all "root" activity by each user.*
2. Objective	Define the objective of the original control; identify the objective met by the compensating control.	*The objective of requiring unique logins is twofold. First, it is not considered acceptable from a security perspective to share login credentials. Secondly, having shared logins makes it impossible to state definitively that a person is responsible for a particular action.*
3. Identified Risk	Identify any additional risk posed by the lack of the original control.	*Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.*
4. Definition of Compensating Controls	Define the compensating controls and explain how they address the objectives of the original control and the increased risk, if any.	*Company XYZ is going to require all users to log into the servers from their desktops using the SU command. SU allows a user to access the "root" account and perform actions under the "root" account but is able to be logged in the SU-log directory. In this way, each user's actions can be tracked through the SU account.*
7. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	*Company XYZ demonstrates to assessor that the SU command being executed and that those individuals utilizing the command are logged to identify that the individual is performing actions under root privileges*
8. Maintenance	Define process and controls in place to maintain compensating controls.	*Company XYZ documents processes and procedures to ensure SU configurations are not changed, altered, or removed to allow individual users to execute root commands without being individually tracked or logged*

Appendix D: Explanation of Non-Applicability

If "N/A" or "Not Applicable" was entered in the "Special" column, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example: *12.8*	*Cardholder data is never shared with service providers.*