Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire C-VT and Attestation of Compliance

Web-Based Virtual Terminal, No Electronic Cardholder Data Storage

Version 2.0

October 2010

Document Changes

Date	Version	Description
October 28, 2010	2.0	New Self Assessment Questionnaire and Attestation of Compliance for merchants using only web-based virtual terminals. Aligned with PCI DSS v2.0 requirements and testing procedures.

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	Eligible merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation	Eligible merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire C-VT and Attestation	Eligible merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation	Eligible merchants[1]
PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation	Eligible merchants and service providers[1]
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-VT has been developed to address requirements applicable to merchants who process cardholder data only via isolated virtual terminals on personal computers connected to the Internet.

A virtual terminal is web-browser based access to an acquirer, processor or third party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.

These merchants process cardholder data only via a virtual terminal and do not store cardholder data on any computer system. These virtual terminals are connected to the Internet to access a third party that hosts the virtual terminal payment processing function. This third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits cardholder data to authorize and/or settle merchants' virtual terminal payment transactions.

This SAQ option is intended to apply only to merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution.

SAQ C-VT merchants process cardholder data via virtual terminals on personal computers connected to the Internet, do not store cardholder data on any computer system, and may be brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. Such merchants validate compliance by completing SAQ C-VT and the associated Attestation of Compliance, confirming that:

- Your company's only payment processing is done via a virtual terminal accessed by an Internet-connected web browser;
- Your company's virtual terminal solution is provided and hosted by a PCI DSS validated third-party service provider;
- Your company accesses the PCI DSS compliant virtual terminal solution via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment (this can be achieved via a firewall or network segmentation to isolate the computer from other systems);
- Your company's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward);
- Your company's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
- Your company does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
- Your company retains only paper reports or paper copies of receipts; **and**
- Your company does not store cardholder data in electronic format.

This option would never apply to e-commerce merchants.

Each section of this questionnaire focuses on a specific area of security, based on the requirements in the *PCI DSS Requirements and Security Assessment Procedures*. This shortened version of the SAQ includes questions which apply to a specific type of small merchant environment, as defined in the above eligibility criteria. If there are PCI DSS requirements applicable to your environment which are not covered in this SAQ, it may be an indication that this SAQ is not suitable for your environment. Additionally, you must still comply with all applicable PCI DSS requirements in order to be PCI DSS compliant.

PCI DSS Compliance – Completion Steps

1. Assess your environment for compliance with the PCI DSS.
2. Complete the Self-Assessment Questionnaire (SAQ C-VT) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines.*
3. Complete the Attestation of Compliance in its entirety.
4. Submit the SAQ and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

Guidance for Non-Applicability of Certain, Specific Requirements

Exclusion: If you are required to answer SAQ C-VT 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).

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 Appendix D for each "N/A" entry.

Attestation of Compliance, SAQ C-VT

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. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

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

Part 1b. 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. Type of merchant business (check all that apply):

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

List facilities and locations included in PCI DSS review:

Part 2a. Relationships

Does your company have a relationship with one or more third-party agents (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 2b. Transaction Processing

Please provide the following information regarding the Virtual Terminal solution your organization uses:

Name of Virtual Terminal solution Service Provider	Name of Virtual Terminal Solution	Date Virtual Terminal Service Provider Last Validated PCI DSS compliance

Part 2c. Eligibility to Complete SAQ C-VT

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

☐	Merchant's only payment processing is via a virtual terminal accessed by an Internet-connected web browser;
☐	Merchant accesses the virtual terminal via a computer that is isolated in a single location, and is not connected to other locations or systems within your environment;
☐	Merchant's virtual terminal solution is provided and hosted by a PCI DSS validated third party service provider;
☐	Merchant's computer does not have software installed that causes cardholder data to be stored (for example, there is no software for batch processing or store-and-forward)
☐	Merchant's computer does not have any attached hardware devices that are used to capture or store cardholder data (for example, there are no card readers attached);
☐	Merchant does not otherwise receive or transmit cardholder data electronically through any channels (for example, via an internal network or the Internet);
☐	Merchant does not store cardholder data in electronic format (for example, cardholder data is not stored in sales or marketing tools such as CRM); **and**
☐	If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically.

Part 3. PCI DSS Validation

Based on the results noted in the SAQ C-VT 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, 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, 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-VT, 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.

Part 3b. Merchant Acknowledgement

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

Merchant Company Represented ↑

[2] Data encoded in the magnetic stripe or equivalent data on a chip 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 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 or programs	☐	☐	
6	Develop and maintain secure systems and applications	☐	☐	
7	Restrict access to cardholder data by business need to know	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
12	Maintain a policy that addresses information security for all personnel	☐	☐	

Self-Assessment Questionnaire C-VT

Note: *The following questions are numbered according to PCI DSS requirements and testing procedures, as defined in the* PCI DSS Requirements and Security Assessment Procedures *document.*

Date of Completion:

Build and Maintain a Secure Network

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

	PCI DSS Question	Response:	Yes	No	Special*
1.2	Do firewall and router configurations 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*.				
	1.2.1 (a)	Is inbound and outbound traffic restricted to that which is necessary for the cardholder data environment, and are the restrictions documented?	☐	☐	
	(b)	Is all other inbound and outbound traffic specifically denied (for example by using an explicit "deny all" or an implicit deny after allow statement)?	☐	☐	
	1.2.3	Are perimeter firewalls installed between any wireless networks and the cardholder data environment, and are these firewalls configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment?	☐	☐	
1.3	Does the firewall configuration prohibit direct public access between the Internet and any system component in the cardholder data environment, as follows:				
	1.3.3	Are direct connections prohibited for inbound or outbound traffic between the Internet and the cardholder data environment?	☐	☐	
	1.3.5	Is outbound traffic from the cardholder data environment to the Internet explicitly authorized?	☐	☐	
	1.3.6	Is stateful inspection, also known as dynamic packet filtering, implemented (that is, only established connections are allowed into the network)?	☐	☐	

* "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.

	PCI DSS Question	Response:	Yes	No	Special*
1.4	(a) Is personal firewall software installed and active 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?		☐	☐	
	(b) Is the personal firewall software configured to specific standards, and not alterable by mobile and/or employee-owned computer users?		☐	☐	

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

	PCI DSS Question	Response:	Yes	No	Special*
2.1	Are vendor-supplied defaults always changed before installing a system on the network? *Vendor-supplied defaults Include but are not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.*		☐	☐	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, are defaults changed as follows:				
	(a) Are encryption keys changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions?		☐	☐	
	(b) Are default SNMP community strings on wireless devices changed?		☐	☐	
	(c) Are default passwords/passphrases on access points changed?		☐	☐	
	(d) Is firmware on wireless devices updated to support strong encryption for authentication and transmission over wireless networks?		☐	☐	
	(e) Are other security-related wireless vendor defaults changed, if applicable?		☐	☐	
2.2.2	(a) Are only necessary services, protocols, daemons, etc. enabled as required for the function of the system (services and protocols not directly needed to perform the device's specified function are disabled)?		☐	☐	

* "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

	PCI DSS Question	Response:	Yes	No	Special*
	3.2.2	The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance?	☐	☐	
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.*		☐	☐	

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

	PCI DSS Question	Response:	Yes	No	Special*
4.1	(a) Are strong cryptography and security protocols, such as SSLTLS, SSH 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 include but are not limited to the Internet, wireless technologies, Global System for Mobile communications (GSM), and General Packet Radio Service (GPRS).*		☐	☐	
	(b) Are only trusted keys and/or certificates accepted?		☐	☐	
	(e) For SSL/TLS implementations: • Does HTTPS appear as part of the browser Universal Record Locator (URL)? • Is cardholder data only required when HTTPS appears in the URL?		☐	☐	
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?		☐	☐	

* "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

	PCI DSS Question	Response:	Yes	No	Special*
5.1	Is anti-virus software deployed on all systems 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 (for example, viruses, Trojans, worms, spyware, adware, and rootkits)?		☐	☐	
5.2	Is all anti-virus software current, actively running, and generating audit logs, as follows:				
	(a) Does the anti-virus policy require updating of anti-virus software and definitions?		☐	☐	
	(c) Are automatic updates and periodic scans enabled?		☐	☐	
	(d) Are all anti-virus mechanisms generating audit logs, and are logs retained in accordance with PCI DSS Requirement 10.7?		☐	☐	

Requirement 6: Develop and maintain secure systems and applications

	PCI DSS Question	Response:	Yes	No	Special*
6.1	(a) Are all system components and software protected from known vulnerabilities by having the latest vendor-supplied security patches installed?		☐	☐	
	(b) Are critical security patches installed within one month of release?		☐	☐	

* "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

	PCI DSS Question	Response:	Yes	No	Special*
7.1	Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:				
7.1.1	Are access rights for privileged user IDs restricted to least privileges necessary to perform job responsibilities?		☐	☐	
7.1.2	Are privileges assigned to individuals based on job classification and function (also called "role-based access control" or RBAC)?		☐	☐	

Requirement 9: Restrict physical access to cardholder data

	PCI DSS Question	Response:	Yes	No	Special*
9.6	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? *For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data*		☐	☐	
9.7	(a) Is strict control maintained over the internal or external distribution of any kind of media?		☐	☐	
	(b) Do controls include the following:				
9.7.1	Is media classified so the sensitivity of the data can be determined?		☐	☐	
9.7.2	Is media sent by secured courier or other delivery method that can be accurately tracked?		☐	☐	
9.8	Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media (especially when media is distributed to individuals)?		☐	☐	
9.9	Is strict control maintained over the storage and accessibility of media?		☐	☐	

* "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.

	PCI DSS Question	Response:	Yes	No	Special*
9.10	Is all media destroyed when it is no longer needed for business or legal reasons?		☐	☐	
	Is destruction performed as follows:				
9.10.1	(a) Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?		☐	☐	
	(b) Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a “to-be-shredded” container has a lock preventing access to its contents.)		☐	☐	

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

	PCI DSS Question	Response:	Yes	No	Special*
12.1	Is a security policy established, published, maintained, and disseminated to all relevant personnel?? *For the purposes of Requirement 12, "personnel" refers to full-time part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the entity's site or otherwise have access to the company's site cardholder data environment.*		☐	☐	
12.1.3	Is the information security policy reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment?		☐	☐	
12.3	(a) Are usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], e-mail, and Internet usage) developed to define proper use of these technologies for all personnel, and require the following:				
12.3.1	Explicit approval by authorized parties to use the technologies?		☐	☐	
12.3.3	A list of all such devices and personnel with access?		☐	☐	
12.3.5	Acceptable uses of the technologies?		☐	☐	
12.4	Do the security policy and procedures clearly define information security responsibilities for all personnel?		☐	☐	
12.5	Are the following information security management responsibilities formally 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	(a) Is a formal security awareness program in place to make all personnel aware of the importance of cardholder data security?		☐	☐	

* "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.

	PCI DSS Question	Response:	Yes	No	Special*
12.8	If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows:				
12.8.1	Is a list of service providers maintained?		☐	☐	
12.8.2	Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possesses?		☐	☐	
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?		☐	☐	
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status, at least annually?		☐	☐	

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.*
5. 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*
6. 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.*