Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire B
and Attestation of Compliance

Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals

© 2006-2017

© 2006-2017

Completing the Self-Assessment Questionnaire

For each question, there is a choice of status regarding that requirement. Only one response should be selected for each question.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the self-assessment with the

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Part 2b. Description of

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
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 after authorization?	Examine data sources including:	☐	☐	☐	☐
		☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

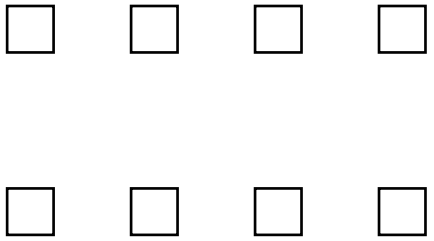
Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Question		Expected Testing	Response (Check one response for each question)			
			Yes	Yes with CCW	No	N/A
4.2	(b) Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies?	Review policies and procedures	☐	☐	☐	☐

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Implement Strong Access Control Measures

Requirement 7 :



© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

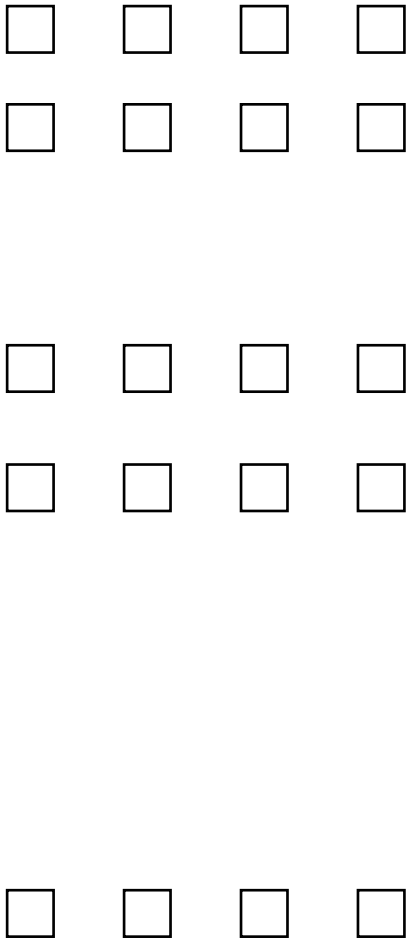
Requirement 9: Restrict physical access to cardholder data

PCI DSS Question	Expected Testing	Response (Check one response for each question)			
		Yes	Yes with CCW	No	
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐
		☐	☐	☐	☐

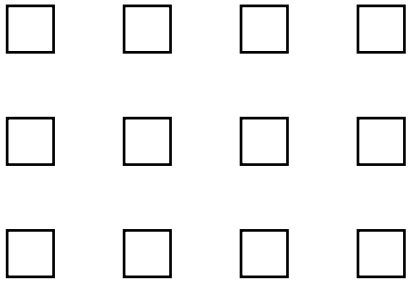
© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

PCI DSS Question	Expected Testing	Response (Check one response for each

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.



© 2006-2017



© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix B: Compensating Controls Worksheet

Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked.

Note: *Only companies that have undertaken a risk analysis and have legitimate technological or*

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Appendix C: Explanation of Non-Applicability

If the "N/A" (Not Applicable) column was checked in the questionnaire, use this worksheet to explain why the related requirement is not applicable to your organization.

Requirement	Reason Requirement is Not Applicable
Example:	
3.4	Cardholder data is never stored electronically

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Part 3a. Acknowledgement of Status (continued)	
☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed by the PCI SSC Approved Scanning Vendor *(ASV Name)*

Part 3b. Merchant Attestation

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

Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.

Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate t for each requirement. If you o may be required to provide the date your Company expects to 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.

PCI DSS Requirement*	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If selected for any Requirement)
		YES	NO	
3	Protect stored cardholder data	☐	☐	
4	Encrypt transmission of cardholder data across open, public networks	☐	☐	
7	Restrict access to cardholder			

© 2006-2017 PCI Security Standards Council, LLC. All Rights Reserved.