



Payment Card Industry (PCI)  
Data Security Standard

# **Self-Assessment Questionnaire A and Attestation of Compliance**

---

**No Electronic Storage, Processing, or  
Transmission of Cardholder Data**

**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

---

<b>Document Changes</b> .....	2
<b>PCI Data Security Standard: Related Documents</b> .....	4
<b>Before You Begin</b> .....	5
<b>Completing the Self-Assessment Questionnaire</b> .....	5
<b>PCI DSS Compliance – Completion Steps</b> .....	5
<b>Guidance for Non-Applicability of Certain, Specific Requirements</b> .....	5
<b>Attestation of Compliance, SAQ A—Merchant Version</b> .....	6
<b>Self-Assessment Questionnaire A</b> .....	9
<b>Implement Strong Access Control Measures</b> .....	9
Requirement 9: Restrict physical access to cardholder data.....	9
<b>Maintain an Information Security Policy</b> .....	10
Requirement 12: Maintain a policy that addresses information security for employees and contractors.....	10
<b>Appendix A: (not used)</b> .....	11
<b>Appendix B: Compensating Controls</b> .....	12
<b>Appendix D: Explanation of Non-Applicability</b> .....	13

## 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
<i>PCI Data Security Standard Requirements and Security Assessment Procedures</i>	All merchants and service providers
<i>Navigating PCI DSS: Understanding the Intent of the Requirements</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Guidelines and Instructions</i>	All merchants and service providers
<i>PCI Data Security Standard: Self-Assessment Questionnaire A and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire B and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire C and Attestation</i>	Merchants <sup>1</sup>
<i>PCI Data Security Standard: Self-Assessment Questionnaire D and Attestation</i>	Merchants <sup>1</sup> and all service providers
<i>PCI Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms</i>	All merchants and service providers

<sup>1</sup>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 A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises.

These merchants, defined as SAQ Validation Type 1 here and in the *PCI DSS Self-Assessment Questionnaire Instructions and Guidelines*, do not store cardholder data in electronic format and do not process or transmit any cardholder data on their premises. Such merchants must validate compliance by completing SAQ A and the associated Attestation of Compliance, confirming that:

- Your company handles only card-not-present (e-commerce or mail/telephone-order) transactions;
- Your company does not store, process, or transmit any cardholder data on your premises, but relies entirely on third party service provider(s) to handle these functions;
- Your company has confirmed that the third party service provider(s) handling storage, processing, and/or transmission of cardholder data is PCI DSS compliant;
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically; **and**
- Your company does not store any cardholder data in electronic format.

**This option would never apply to merchants with a face-to-face POS environment.**

### PCI DSS Compliance – Completion Steps

1. Complete the Self-Assessment Questionnaire (SAQ A) according to the instructions in the *Self-Assessment Questionnaire Instructions and Guidelines*.
2. Complete the Attestation of Compliance in its entirety.
3. 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

**Non-Applicability:** 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 A—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:	EMP Merchandising GmbH	DBA(S):			
Contact Name:	Oliver Schepers	Title:			
Telephone:	05919143235	E-mail:	oliver.schepers@emp.de		
Business Address:	Darmer Esch 70a	City:	Lingen		
State/Province:		Country:	Deutschland	ZIP:	49811
URL:	www.emp.de				

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

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

List facilities and locations included in PCI DSS review:      Lingen/Deutschland

#### 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. Eligibility to Complete SAQ A

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

<input checked="" type="checkbox"/>	Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions;
<input checked="" type="checkbox"/>	The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant;
<input checked="" type="checkbox"/>	Merchant does not store cardholder data in electronic format; <b>and</b>
<input checked="" type="checkbox"/>	If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically.

## Part 3. PCI DSS Validation

Based on the results noted in the SAQ A dated 13.01.10, *EMP Merchandising GmbH* 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 *EMP Merchandising GmbH* 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 *EMP Merchandising GmbH* 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:

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire A, Version 1.2, was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.

## Part 3b. Merchant Acknowledgement

	13.01.10
<i>Signature of Merchant Executive Officer</i> ↑	<i>Date</i> ↑
<i>Merchant Executive Officer Name</i> ↑	<i>Title</i> ↑
EMP Merchandising GmbH	
<i>Merchant Company Represented</i> ↑	

## 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	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security	<input checked="" type="checkbox"/>	<input type="checkbox"/>	



## Self-Assessment Questionnaire A

Date of Completion: 13.01.10

### Implement Strong Access Control Measures

#### **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?		<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"/>	
9.7 (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"/>	
9.10	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"/>	

\* "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*
12.8	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 type="checkbox"/>	<input type="checkbox"/>	na
12.8.1	A list of service providers is maintained.		<input type="checkbox"/>	<input type="checkbox"/>	na
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 type="checkbox"/>	<input type="checkbox"/>	na
12.8.3	There is an established process for engaging service providers, including proper due diligence prior to engagement.		<input type="checkbox"/>	<input type="checkbox"/>	na
12.8.4	A program is maintained to monitor service providers' PCI DSS compliance status.		<input type="checkbox"/>	<input type="checkbox"/>	na

\* "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)**

## 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. Twofactor 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 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
12.8	<i>Es gibt keine Dienstleister, die auf Kreditkarteninhaberdaten zugreifen können</i>
12.8.1	<i>Es gibt keine Dienstleister, die auf Kreditkarteninhaberdaten zugreifen können</i>
12.8.2	<i>Es gibt keine Dienstleister, die auf Kreditkarteninhaberdaten zugreifen können</i>
12.8.3	<i>Es gibt keine Dienstleister, die auf Kreditkarteninhaberdaten zugreifen können</i>
12.8.4	<i>Es gibt keine Dienstleister, die auf Kreditkarteninhaberdaten zugreifen können</i>