



Payment Card Industry (PCI)

Data Security Standard

**Self-Assessment Questionnaire
A**

and Attestation Of Compliance

**Card-not-present Merchants, All Cardholder
Data Functions Fully Outsourced**

For use with PCI DSS Version 3.2.1

Revision 1.0

June 2018

Document changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.0 to 3.1.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.1 to 3.2. Requirements added from PCI DSS v3.2 Requirements 2, 8, and 12.
January 2017	3.2	1.1	Updated Document Changes to clarify requirements added in the April 2016 update. Added note to Before You Begin section to clarify intent of inclusion of PCI DSS Requirements 2 and 8.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see PCI DSS - Summary of Changes from PCI DSS Version 3.2 to 3.2.1. Added Requirement 6.2 from PCI DSS v3.2.1.

Table of contents

Document changes	2
Before you Begin	4
PCI DSS Compliance-Completion Steps	4
Understanding the Self-Assessment Questionnaire	5
Completing the Self-Assessment Questionnaire	5
Guidance for Non-Applicability of Certain, Specific Requirements	6
Legal Exception	6
Section 1: Assessment Information	7
Section 2: Self-Assessment Questionnaire A	12
Build and Maintain a Secure Network and Systems	12
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	12
Maintain a Vulnerability Management Program	13
Requirement 6: Develop and maintain secure systems and applications	13
Implement Strong Access Control Measures	14
Requirement 8: Identify and authenticate access to system components	14
Requirement 9: Restrict physical access to cardholder data	14
Maintain an Information Security Policy	15
Requirement 12: Maintain a policy that addresses information security for all personnel.	15
Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers	14
Appendix B: Compensating Controls Worksheet	15
Appendix C: Explanation of Non-Applicability	16
Annotation	17
Section 3: Validation and Attestation Details	18

Before you Begin

SAQ A has been developed to address requirements applicable to merchants whose cardholder data functions are completely outsourced to validated third parties, where the merchant retains only paper reports or receipts with cardholder data.

SAQ A merchants may be either e-commerce or mail/telephone-order merchants (card-not-present), and do not store, process, or transmit any cardholder data in electronic format on their systems or premises.

SAQ A merchants confirm that, for this payment channel:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
- Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.

Additionally, for e-commerce channels:

- All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

This SAQ is not applicable to face-to-face channels.

This shortened version of the SAQ includes questions that 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 that 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.

Note: For this SAQ, PCI DSS Requirements that address the protection of computer systems (for example, Requirements 2 and 8) apply to e-commerce merchants that redirect customers from their website to a third party for payment processing, and specifically to the merchant webserver upon which the redirection mechanism is located. Mail order/telephone order (MOTO) or e-commerce merchants that have completely outsourced all operations (where there is no redirection mechanism from the merchant to the third party) and therefore do not have any systems in scope for this SAQ, would consider these requirements to be "not applicable." Refer to guidance on the following pages for how to report requirements that are not applicable.

PCI DSS Self-Assessment Completion Steps

1. Identify the applicable SAQ for your environment - refer to the Self-Assessment Questionnaire Instructions and Guidelines document on PCI SSC website for information.
2. Confirm that your environment is properly scoped and meets the eligibility criteria for the SAQ you are using (as defined in Part 2g of the Attestation of Compliance).
3. Assess your environment for compliance with applicable PCI DSS requirements.
4. Complete all sections of this document:
 - Section 1 (Part 1 & 2 of the AOC) - Assessment Information and Executive Summary.
 - Section 2 - PCI DSS Self-Assessment Questionnaire (SAQ A).
 - Section 3 (Parts 3 & 4 of the AOC) - Validation and Attestation Details and Action Plan for Non-Compliant Requirements (if applicable)
5. Submit the SAQ and Attestation of Compliance (AOC), along with any other requested documentation - such as ASV scan reports - to your acquirer, payment brand or other requester.

Understanding the Self-Assessment Questionnaire

The questions contained in the "PCI DSS Question" column in this self-assessment questionnaire are based on the requirements in the PCI DSS.

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided to assist with the assessment process. An overview of some of these resources is provided below:

Document	Includes:
PCI DSS (PCI Data Security Standard Requirements and Security Assessment Procedures)	<ul style="list-style-type: none"> • Guidance on Scoping • Guidance on the intent of all PCI DSS Requirements • Details of testing procedures • Guidance on Compensating Controls
SAQ Instructions and Guidelines documents	<ul style="list-style-type: none"> • Information about all SAQs and their eligibility criteria • How to determine which SAQ is right for your organization
PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms	<ul style="list-style-type: none"> • Descriptions and definitions of terms used in the PCI DSS and self-assessment questionnaires

These and other resources can be found on the PCI SSC website (www.pcisecuritystandards.org). Organizations are encouraged to review the PCI DSS and other supporting documents before beginning an assessment.

Completing the Self-Assessment Questionnaire

For each question, there is a choice of responses to indicate your company's status regarding that requirement. **Only one response should be selected for each question.**

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
Yes	The expected testing has been performed, and all elements of the requirement have been met as stated.
Yes with CCW (Compensating Control Worksheet)	<p>The expected testing has been performed, and the requirement has been met with the assistance of a compensating control.</p> <p>All responses in this column require completion of a Compensating Control Worksheet (CCW) in Appendix B of the SAQ.</p> <p>Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS.</p>
No	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
N/A (Not Applicable)	<p>The requirement does not apply to the organization's environment. (See Guidance for Non-Applicability of Certain, Specific Requirements below for examples.)</p> <p>All responses in this column require a supporting explanation in Appendix C of the SAQ.</p>

Guidance for Non-Applicability of Certain, Specific Requirements

If any requirements are deemed not applicable to your environment, select the "N/A" option for that specific requirement, and complete the "Explanation of Non-Applicability" worksheet in Appendix C for each "N/A" entry.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, check the "No" column for that requirement and complete the relevant attestation in Part 3.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information			
Part 1a. Merchant Organisation Information			
Company Name:	Grace Software Inc	DBA (doing business as):	GraceSoft
Contact Name:	Gideon Stanley	Title:	CEO
ISA Name(s) (if applicable):		Title:	
Telephone:	713-981-5300	E-mail:	sysadmin2@gracesoft.com
Business Address:	7310 Cortez Road, Richmond		
	TEXAS - 77469		
Country:	USA		
URL:	www.gracesoft.com		

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

Company Name:			
Lead QSA Contact Name:		Title:	
Telephone:		Email:	
Business Address:			
Country:			
URL:			

Part 2. Executive Summary

Part 2a. Type of Merchant Business (check all that apply)

<input type="checkbox"/> Retailer	<input type="checkbox"/> Telecommunications	<input type="checkbox"/> Grocery and Supermarkets
<input type="checkbox"/> Petroleum	<input type="checkbox"/> E-Commerce	<input type="checkbox"/> Mail order/telephone order (MOTO)
<input type="checkbox"/> Others (please specify):		

<p>What types of payment channels does your business serve?</p> <p><input type="checkbox"/> Mail order/telephone order (MOTO)</p> <p><input checked="" type="checkbox"/> E-Commerce</p> <p><input type="checkbox"/> Card-present (face-to-face)</p>	<p>Which payment channels are covered by this SAQ?</p> <p><input type="checkbox"/> Mail order/telephone order (MOTO)</p> <p><input checked="" type="checkbox"/> E-Commerce</p> <p><input type="checkbox"/> Card-present (face-to-face)</p>
---	--

Note: If your organization has a payment channel or process that is not covered by this SAQ, consult your acquirer or payment brand about validation for the other channels.

Part 2b. Description of Payment Card Business

How and in what capacity does your business store, process and/or transmit cardholder data?

Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)

Part 2d. Payment Application

Does the organization use one or more Payment Applications?

 Yes No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed	PA-DSS Listing Expiry date (if applicable)
			<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

Part 2e. Description of Environment

Provide a **high-level** description of the environment covered by this assessment.

For example:

- Connections into and out of the cardholder data environment (CDE).
- Critical system components within the CDE, such as POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.

Does your business use network segmentation to affect the scope of your PCI DSS environment? (Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)

 Yes No

Part 2f. Third-Party Service Providers

Does your company use a Qualified Integrator & Reseller (QIR)?	<input type="checkbox"/>
If Yes:	Yes
Name of QIR Company:	<input checked="" type="checkbox"/>
QIR Individual Name:	No
Description of services provided by QIR:	

Does your company share cardholder data with any third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.)?	<input checked="" type="checkbox"/>
	Yes
	<input type="checkbox"/>
	No

If Yes:	
Name of service provider:	Description of services provided:
Microsoft Corp	Hosting
Moneris Solutions Corporation / Moneris Solutions Inc. Stripe Inc CyberSource (including Authorize.Net Managed Hosting and K.K.) PayPal	Payment Processing
GraceSoft	Shopping Cart

Note: Requirement 12.8 applies to all entities in this list.

Part 2g. Eligibility to Complete SAQ A

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

<input checked="" type="checkbox"/>	Merchant accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
<input checked="" type="checkbox"/>	All processing of cardholder data is entirely outsourced to PCI DSS validated third-party service providers;
<input checked="" type="checkbox"/>	Merchant does not electronically store, process, or transmit any cardholder data on merchant systems or premises, but relies entirely on a third party(s) to handle all these functions;
<input checked="" type="checkbox"/>	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
<input checked="" type="checkbox"/>	Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically.
<input checked="" type="checkbox"/>	Additionally, for e-commerce channels: All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s).

Section 2: Self-Assessment Questionnaire A

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.

Self-assessment completion date: 06/13/2023

Build and Maintain a Secure Network and Systems

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

PCI DSS Question		Response: (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
2.1(a)	<p>Are vendor-supplied defaults always changed before installing a system on the network?</p> <p><i>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.</i></p>				
2.1(b)	<p>Are unnecessary default accounts removed or disabled before installing a system on the network?</p>				

Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Response: (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
6.2(a)	Are all system components and software protected from known vulnerabilities by installing applicable vendor-supplied security patches?				
6.2(b)	Are critical security patches installed within one month of release? <i>Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.</i>				

Implement Strong Access Control Measures

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Response: (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
8.1.1	Are all users assigned a unique ID before allowing them to access system components or cardholder data?				
8.1.3	Is access for any terminated users immediately deactivated or removed?				
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"> • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric 				
8.2.3 (a)	Are user password parameters configured to require passwords/passphrases meet the following? <ul style="list-style-type: none"> • A minimum password length of at least seven characters • Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.				
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: <ul style="list-style-type: none"> • Generic user IDs and accounts are disabled or removed; • Shared user IDs for system administration activities and other critical functions do not exist; and • Shared and generic user IDs are not used to administer any system components? 				

Requirement 9: Restrict physical access to cardholder data

PCI DSS Question		Response: (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
9.5	Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)? <i>For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data.</i>				

9.6(a)	Is strict control maintained over the internal or external distribution of any kind of media?				
9.6(b)	Do controls include the following:				
9.6.1	Is media classified so the sensitivity of the data can be determined?				
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?				
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?				
9.7	Is strict control maintained over the storage and accessibility of media?				
9.8(a)	Is all media destroyed when it is no longer needed for business or legal reasons?				
9.8(c)	Is media destruction performed as follows:				
9.8.1 (a)	Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?				
9.8.1 (b)	Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?				

Maintain an Information Security Policy

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

Note: 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.

PCI DSS Question		Response: (Check one response for each question)			
		Yes	Yes with CCW	No	N/A
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:				
12.8.1	Is a list of service providers maintained, including a description of the service(s) provided?				
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 possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment? <i>Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.</i>				
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?				
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?				
12.10.1 (a)	Has an incident response plan been created to be implemented in the event of system breach?				

Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

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 documented business constraints can consider the use of compensating controls to achieve compliance.

Refer to Appendices B, C, and D of PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

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.	

S

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

Annotation

MIDs/ Accounts covered by this Attestation-of-Compliance

Mid / Account	Company name	Address Line 1
merchant_720107	Grace Software Inc	7310 Cortez Rd, Richmond, TX 77469

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation:

Based on the results noted in the SAQ A dated 06/13/2023, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document as of 06/13/2023 (**check one**):


<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby Gracesoft has demonstrated full compliance with the PCI DSS.</p>
<input type="checkbox"/>	<p>Non-Compliant: Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby Gracesoft has not demonstrated full compliance with the PCI DSS.</p> <p>Target Date for Compliance:</p> <p>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.</p>
<input type="checkbox"/>	<p>Compliant but with Legal exception: One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p>

Part 3a. Acknowledgement of Status

Signatory(s) confirms:
(Check all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire A , Version 3.2.1, 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 PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.
<input checked="" type="checkbox"/>	No evidence of full track data ² , CAV2, CVC2, CID or CVV2 data ³ , or PIN data ⁴ was found on ANY system reviewed during this assessment.

Part 3b. Merchant Attestation

Signature of Merchant Executive Officer 		Date: 6/13/2023
Merchant Executive Officer Name: Gideon Stanley		Title: CEO

Part 3c. QSA Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:	
Signature of Duly Authorized Officer of QSA Company	Date:
Duly Authorized Officer Name:	QSA Company:

Part 3d. ISA Acknowledgement (if applicable)

If a ISA was involved or assisted with this assessment, describe the role performed:	
Signature of ISA	Date:
ISA Name:	Title:

- 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 track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.
- ³ The three- or four-digit value printed by 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.