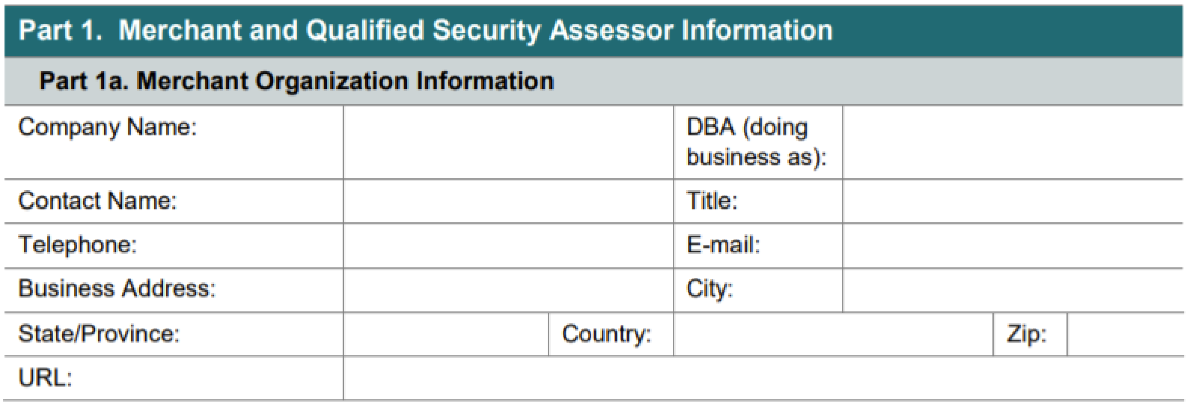
Appendix A - How to Complete the SAQ - A

Once you onboard with the Online Payments product from Airwallex, you will be required to fill out the SAQ-A. Below is some guidance on how to populate the information.

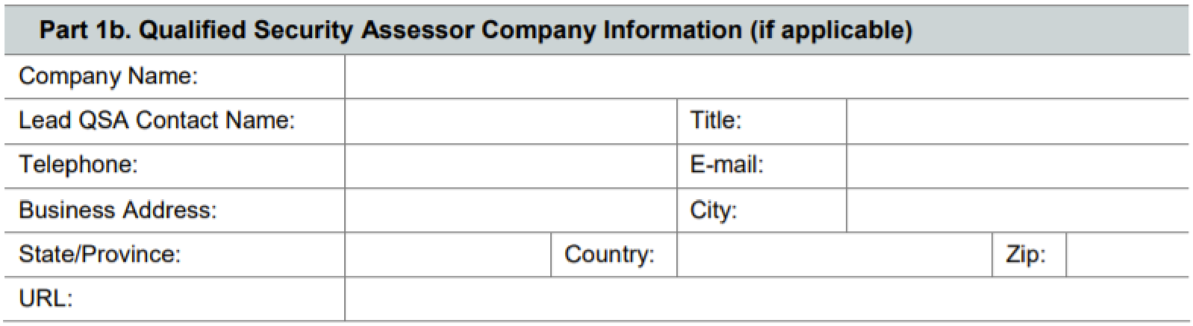


Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

Company Name:		DBA (doing business as):			
Contact Name:		Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		Zip:	
URL:					

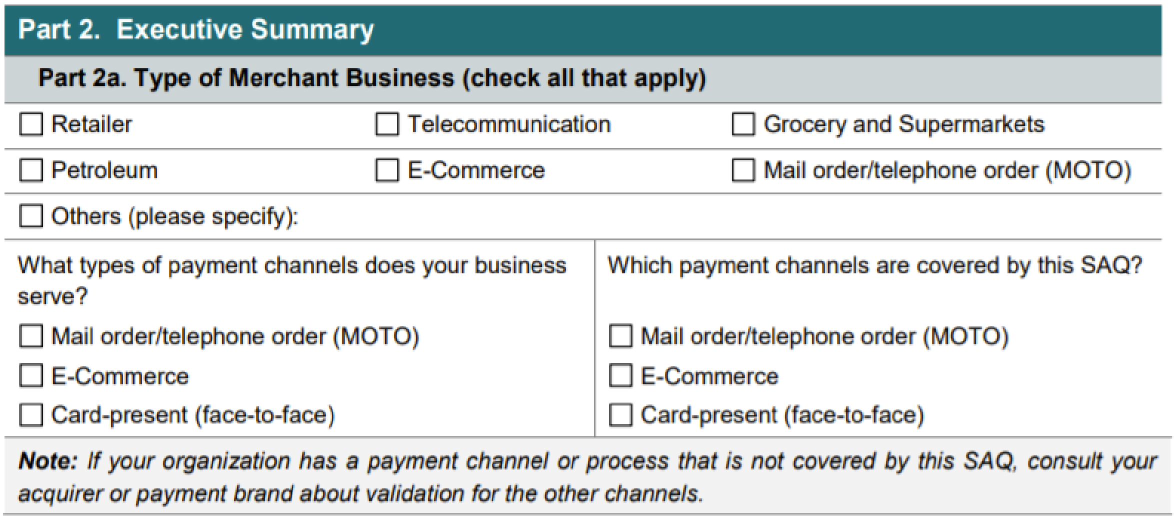
Part 1a. Company Name: Should be consistent with the entity of the merchant, unless otherwise stated in Part2b.
URL: Merchant's official website or the main transaction website.



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 1b. Company Name: If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
Note that Level 1 Merchants must use a Qualified Security Assessor.



Part 2. Executive Summary

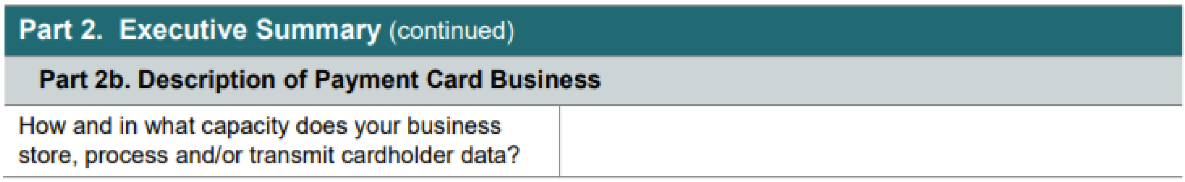
Part 2a. Type of Merchant Business (check all that apply)

□ Retailer	□ Telecommunication	□ Grocery and Supermarkets
□ Petroleum	□ E-Commerce	□ Mail order/telephone order (MOTO)
□ Others (please specify):		

What types of payment channels does your business serve? □ Mail order/telephone order (MOTO) □ E-Commerce □ Card-present (face-to-face)	Which payment channels are covered by this SAQ? □ Mail order/telephone order (MOTO) □ E-Commerce □ Card-present (face-to-face)

***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.*

In the above section, check what is most relevant to your business. In most cases for the SAQ-A form, 'E-Commerce' is the most relevant checkbox.



Part 2. Executive Summary (continued)

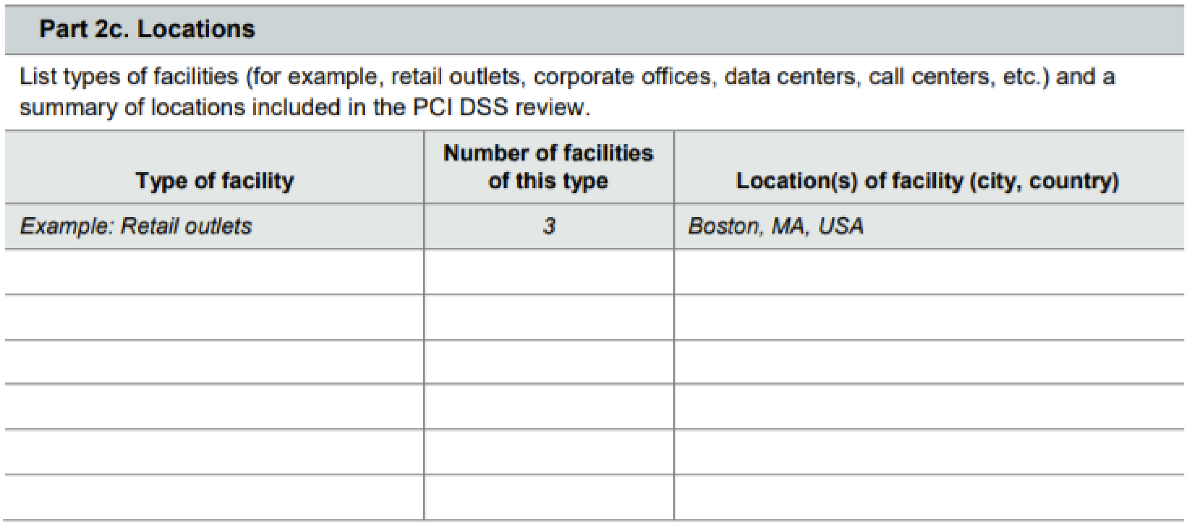
Part 2b. Description of Payment Card Business

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

Part 2(b) The specific process and treatment method of the following links should be clearly described: How to collect, transfer, store and reuse card information: If you are using HostedPaymentPage, Drop-in and Element, it can be described as: "We do not store, process or transmit cardholder data. The cardholder data is collected, stored, and processed via Airwallex hosted payment page/Airwallexdrop-in/Airwallex element."

**If you are collecting the first six and last four memory card numbers you can mentioned this here.*

Describe in detail the payment card environment. This may include the goods and services consumers purchase, how card payments are processed and service providers and how they interact with the payment card environment.

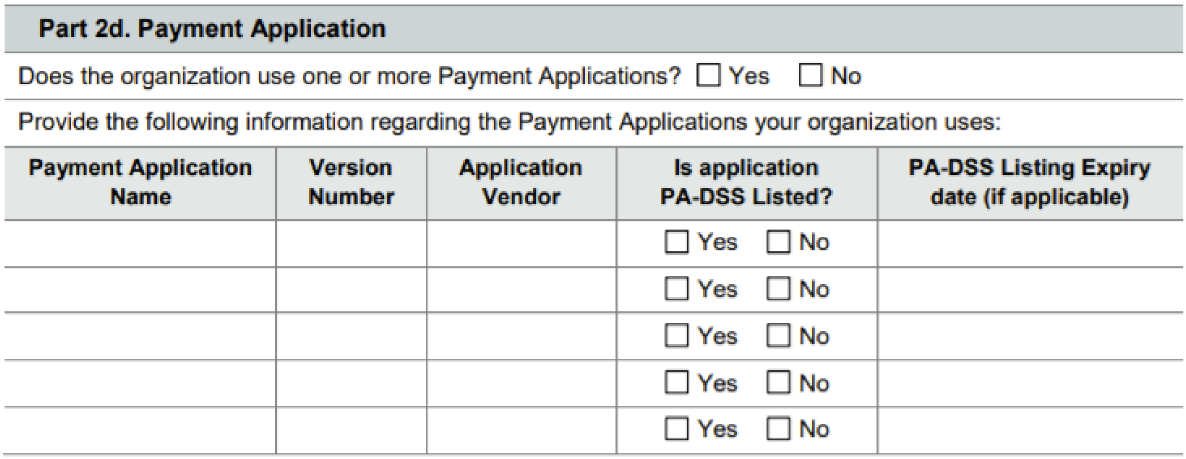


Part 2c. Locations

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)
Example: Retail outlets	*3*	*Boston, MA, USA*

Relates to the facilities for your company. When completing the SAQ A form it will most often be a corporate office, data centre etc as companies filling in this form will typically have e-commerce sales.



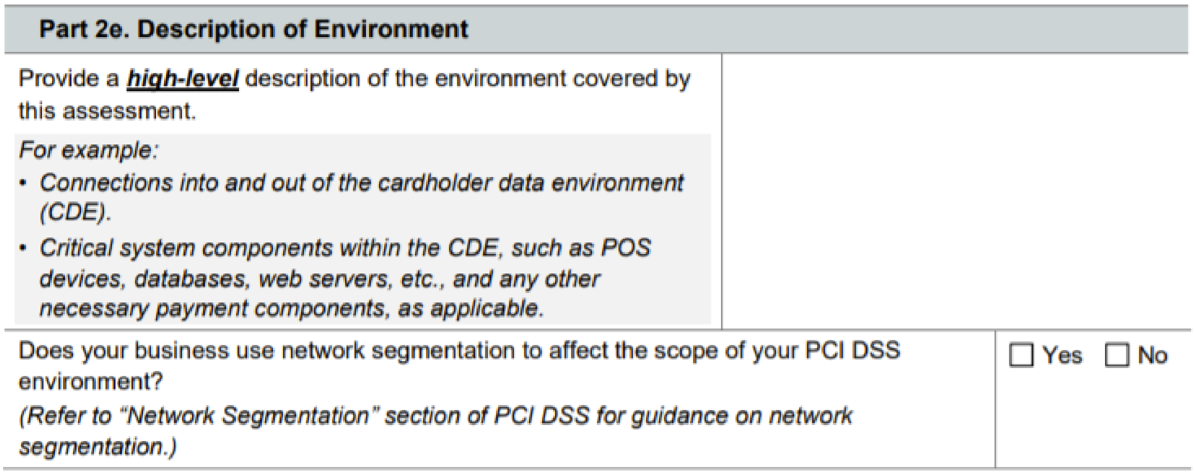
Part 2d. Payment Application

Does the organization use one or more Payment Applications? □ Yes □ No

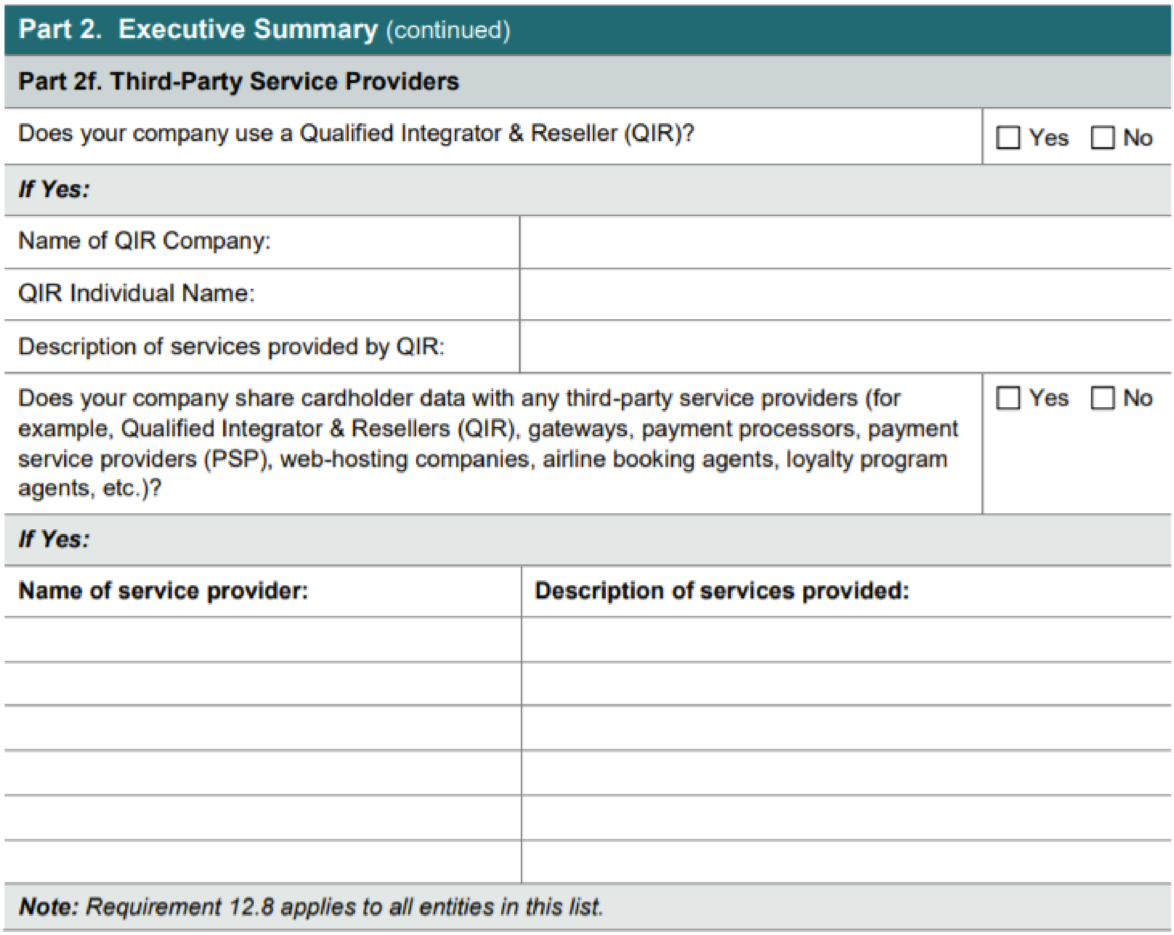
Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	
			□ Yes □ No	

If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true
If not, check NO on the first line above.



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 2. Executive Summary (continued)	
Part 2f. Third-Party Service Providers	
Does your company use a Qualified Integrator & Reseller (QIR)?	□ Yes □ No
If Yes:	
Name of QIR Company:	
QIR Individual Name:	
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.)?	□ Yes □ No
If Yes:	
Name of service provider:	**Description of services provided:**
Note: *Requirement 12.8 applies to all entities in this list.*	

Name of QIR Company: It can be found here: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

Note that you do not need to fill this part unless you collect cardholder data and share to third-party. If you collect cardholder data from Airwallex and shares to other PSP then the PSP should be listed in below form; If the client collects cardholder data from other acquirer and shares to us then we need to be listed.

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:

□	Merchant 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;
□	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;
□	Merchant has confirmed that all third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant; **and**
□	Any cardholder data the merchant 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).

Check all.

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:

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		Expected Testing	Response *(Check one response for each question)*			
			Yes	**Yes with CCW**	**No**	**N/A**
2.1	(a) Are vendor-supplied defaults always changed before installing a system on the network? *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.).*	▪ Review policies and procedures. ▪ Examine vendor documentation. ▪ Observe system configurations and account settings. ▪ Interview personnel.	□	□	□	□
	(b) Are unnecessary default accounts removed or disabled before installing a system on the network?	▪ Review policies and procedures. ▪ Review vendor documentation. ▪ Examine system configurations and account settings. ▪ Interview personnel.	□	□	□	□

Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Question		Expected Testing	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?	▪ Review policies and procedures.	□	□	□	□
	(b) Are critical security patches installed within one month of release?	▪ Review policies and procedures. ▪ Examine system components. ▪ Compare list of security patches installed to recent vendor patch lists.	□	□	□	□

Implement Strong Access Control Measures

Requirement 8: Identify and authenticate access to system components

PCI DSS Question		Expected Testing	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?	▪ Review password procedures. ▪ Interview personnel.	□	□	□	□
8.1.3	Is access for any terminated users immediately deactivated or removed?	▪ Review password procedures. ▪ Examine terminated users accounts. ▪ Review current access lists. ▪ Observe returned physical authentication devices.	□	□	□	□
8.2	In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users? ▪ 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	▪ Review password procedures. ▪ Observe authentication processes.	□	□	□	□
8.2.3	(a) Are user password parameters configured to require passwords/passphrases meet the following? • 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.	▪ Examine system configuration settings to verify password parameters.	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
8.5	Are group, shared, or generic accounts, passwords, or other authentication methods prohibited as follows: ▪ 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?	▪ Review policies and procedures. ▪ Examine user ID lists. ▪ Interview personnel.	□	□	□	□

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	N/A
9.5	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.*	▪ Review policies and procedures for physically securing media. ▪ Interview personnel.	□	□	□	□
9.6	(a) Is strict control maintained over the internal or external distribution of any kind of media?	▪ Review policies and procedures for distribution of media.	□	□	□	□
	(b) Do controls include the following:					
9.6.1	Is media classified so the sensitivity of the data can be determined?	▪ Review policies and procedures for media classification. ▪ Interview security personnel.	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
9.6.2	Is media sent by secured courier or other delivery method that can be accurately tracked?	▪ Interview personnel. ▪ Examine media distribution tracking logs and documentation.	□	□	□	□
9.6.3	Is management approval obtained prior to moving the media (especially when media is distributed to individuals)?	▪ Interview personnel. ▪ Examine media distribution tracking logs and documentation.	□	□	□	□
9.7	Is strict control maintained over the storage and accessibility of media?	▪ Review policies and procedures.	□	□	□	□
9.8	(a) Is all media destroyed when it is no longer needed for business or legal reasons?	▪ Review periodic media destruction policies and procedures.	□	□	□	□
	(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?	▪ Review periodic media destruction policies and procedures. ▪ Interview personnel. ▪ Observe processes.	□	□	□	□
	(b) Are storage containers used for materials that contain information to be destroyed secured to prevent access to the contents?	▪ Examine security of storage containers.	□	□	□	□

Maintain an Information Security Policy

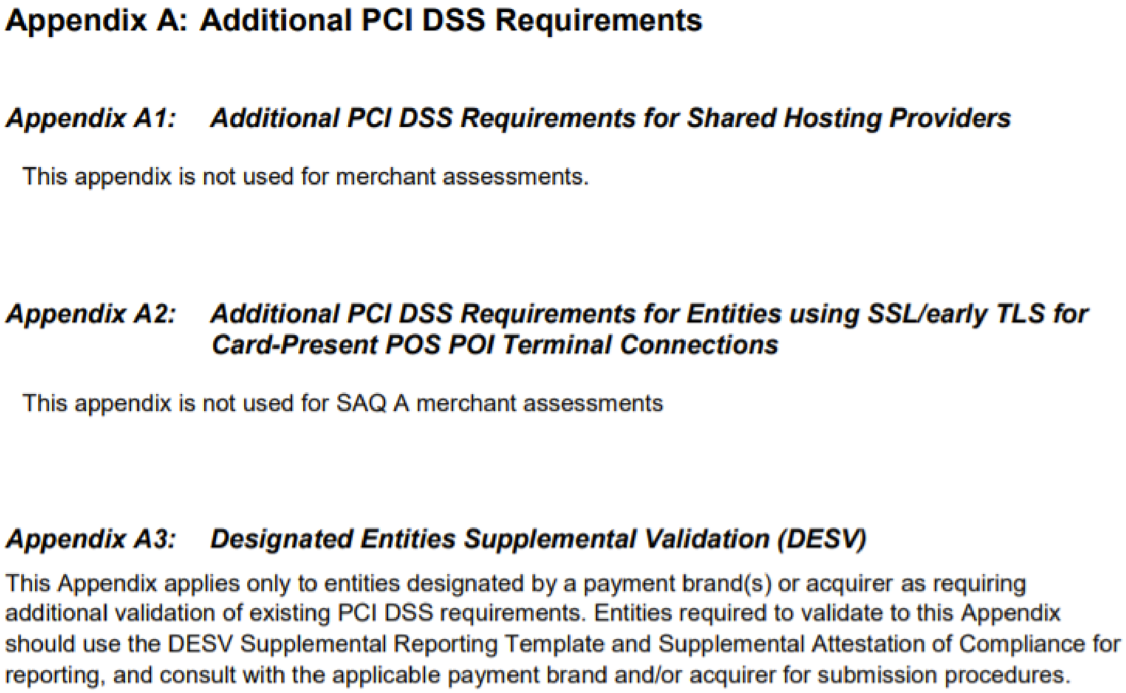
Requirement 12: Maintain a policy that addresses information security for all personnel

***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		Expected Testing	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?	▪ Review policies and procedures. ▪ Observe processes. ▪ Review list of service providers.	□	□	□	□
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? ***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.*	▪ Observe written agreements. ▪ Review policies and procedures.	□	□	□	□
12.8.3	Is there an established process for engaging service providers, including proper due diligence prior to engagement?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	□	□	□	□

PCI DSS Question		Expected Testing	Response *(Check one response for each question)*			
			Yes	Yes with CCW	No	N/A
12.8.4	Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	□	□	□	□
12.8.5	Is information maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity?	▪ Observe processes. ▪ Review policies and procedures and supporting documentation.	□	□	□	□
12.10.1	(a) Has an incident response plan been created to be implemented in the event of system breach?	▪ Review the incident response plan. ▪ Review incident response plan procedures.	□	□	□	□

Self-assessment completion date: Enter date
For Section 2 Merchant needs to complete the questionnaire. There are 12 sections. Where a merchant can respond to the question in the affirmative check 'yes'.
If there are compensating controls please check 'CCW' and add additional information in Appendix B.
If there is any question which is not applicable then check 'N/A' and provide details in Appendix C.



Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

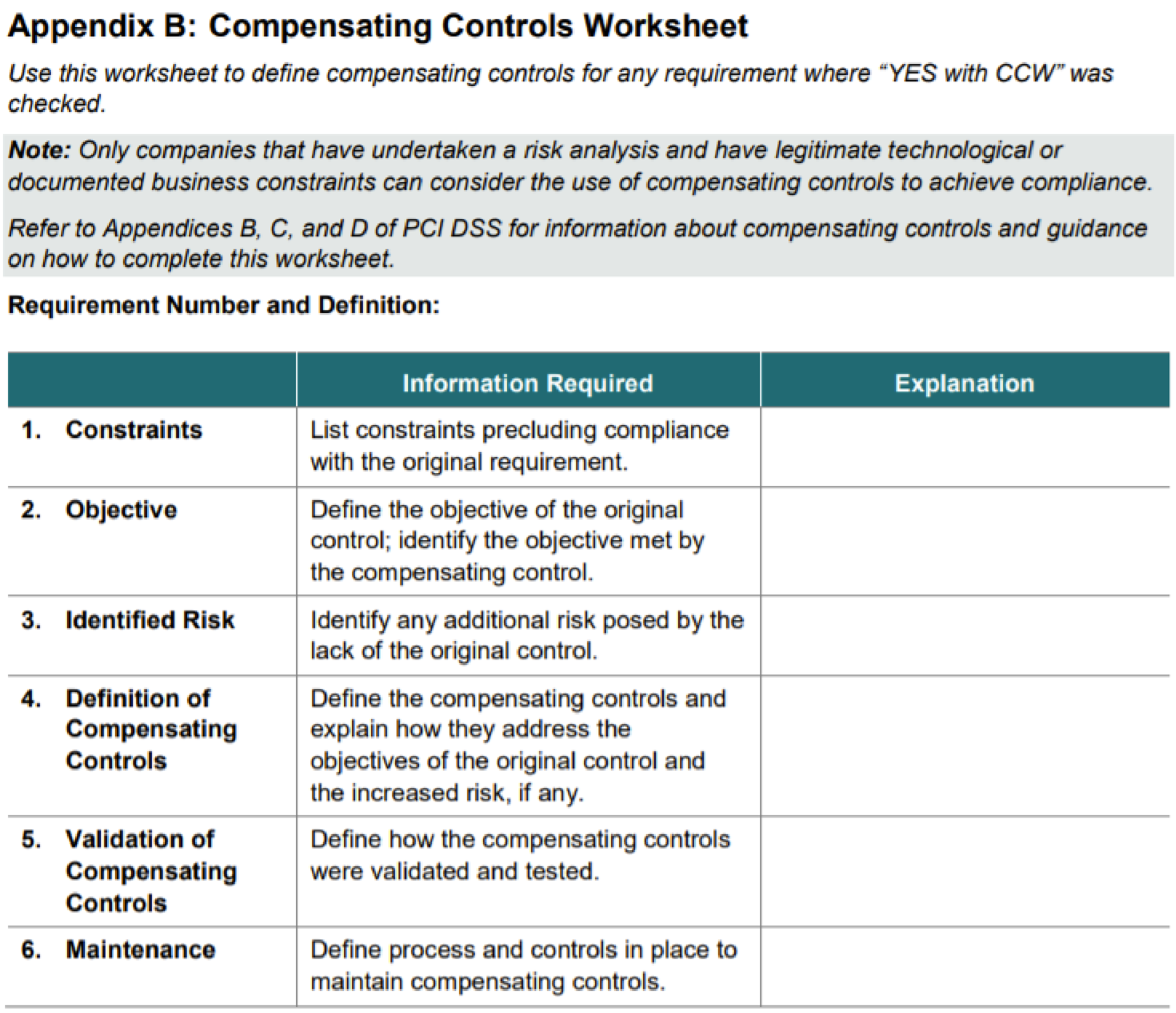
This appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections

This appendix is not used for SAQ A merchant assessments

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting, and consult with the applicable payment brand and/or acquirer for submission procedures.



Appendix B: Compensating Controls Worksheet

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

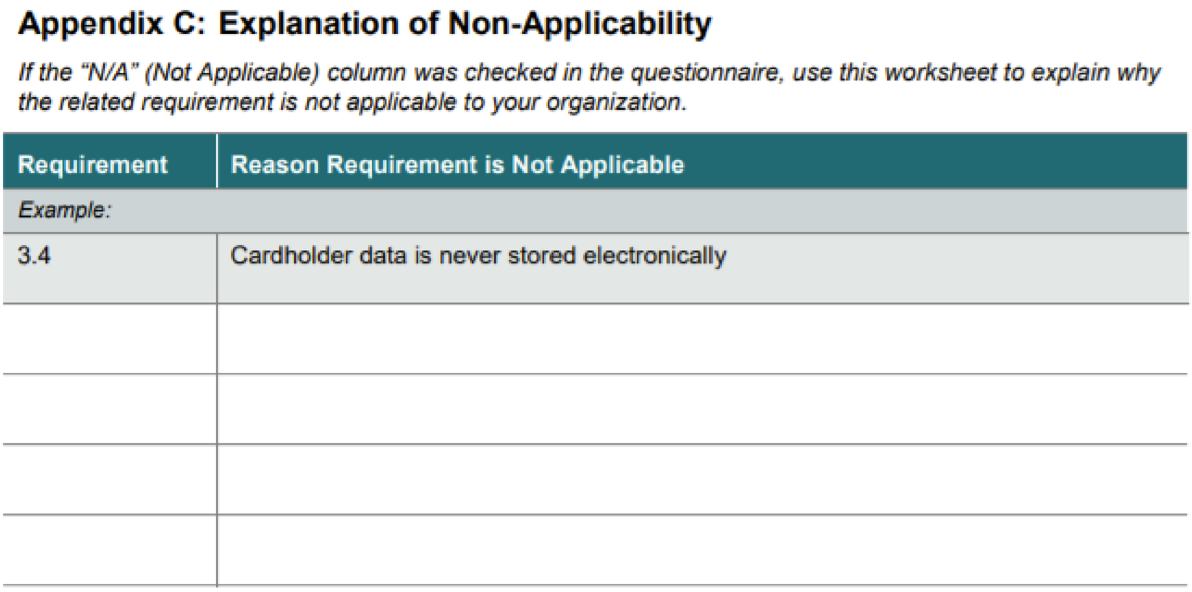
Note: *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.*

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.	

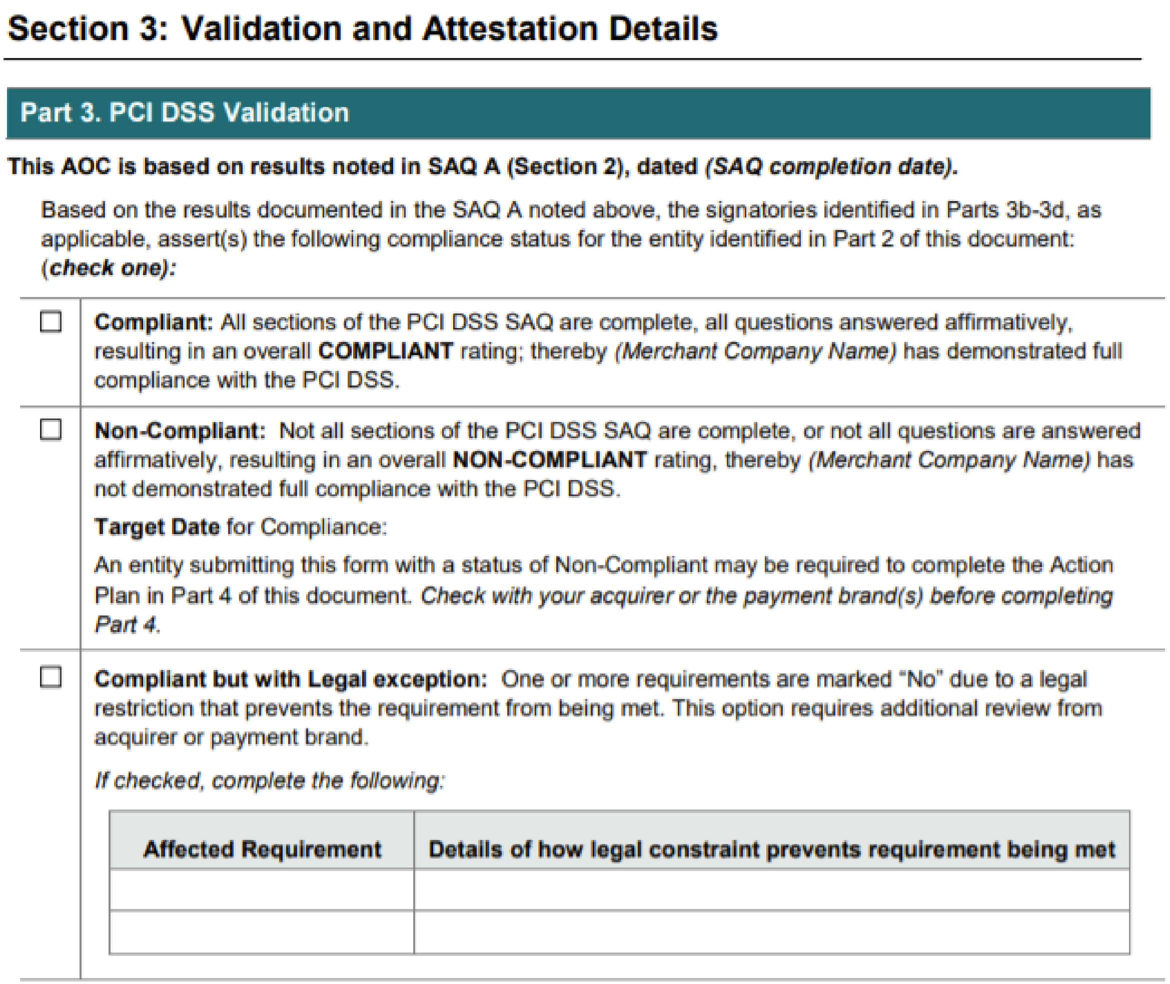
Use this worksheet to define compensating controls for any requirement where "YES with CCW" was checked in ***Section 2 Self Assessment Questionnaire A.***



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



Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ A (Section 2), dated *(SAQ completion date)*.

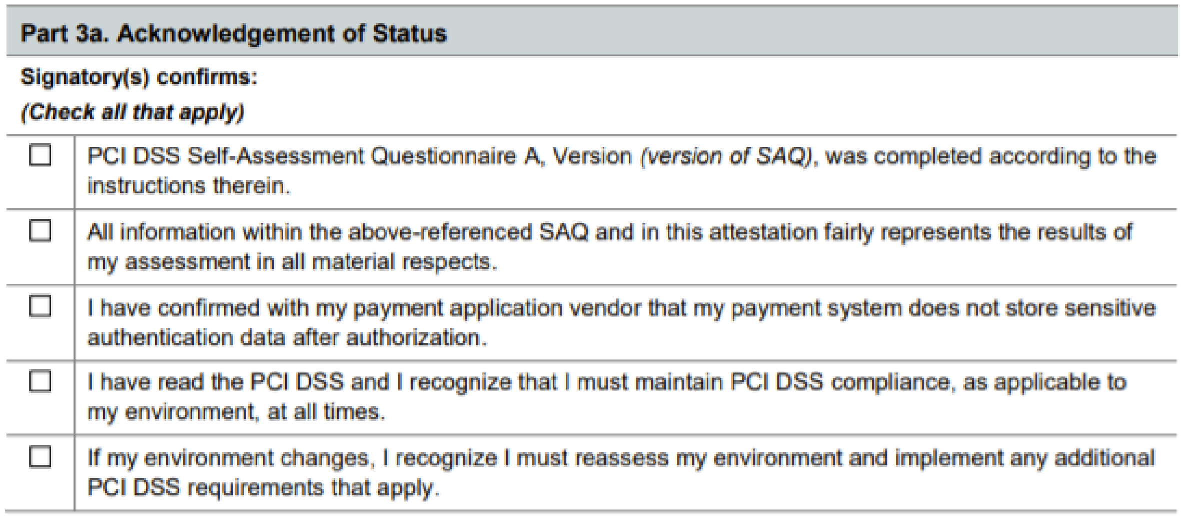
Based on the results documented in the SAQ A noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: (***check one)*:**

□	**Compliant:** All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, 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 DSS SAQ are complete, or not all questions are answered affirmatively, 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.*
□	**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. *If checked, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement being met

(SAQ completion date) replace this with the relevant date.

Compliant: replace (Merchant Company Name) with your Company name.



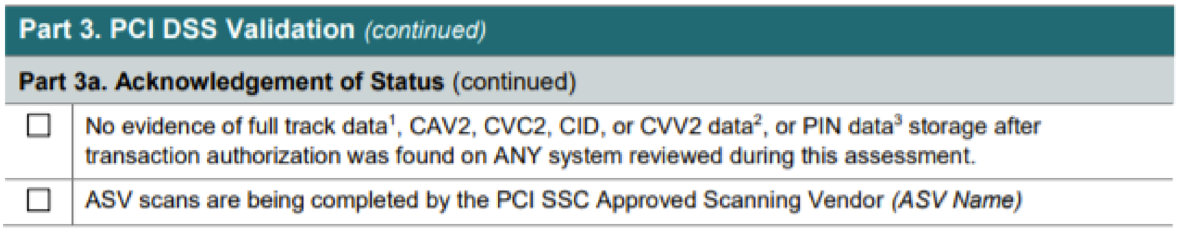
Part 3a. Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

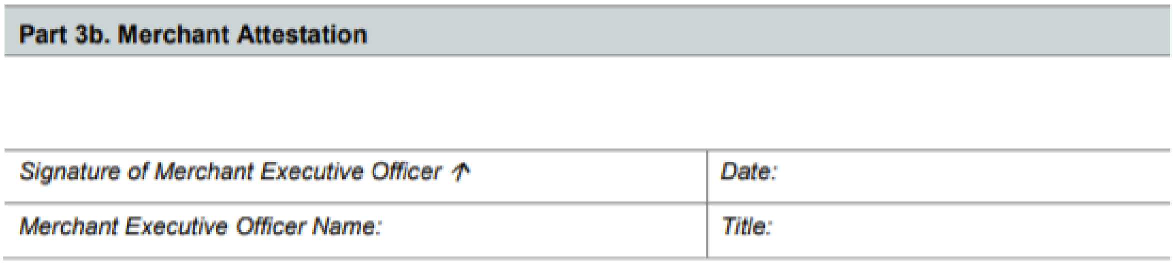
□	PCI DSS Self-Assessment Questionnaire A, Version *(version of SAQ)*, was completed according to the instructions therein.
□	All information within the above-referenced SAQ and in this attestation fairly represents the results of my assessment in all material respects.
□	I have confirmed with my payment 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 PCI DSS compliance, as applicable to my environment, at all times.
□	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

Check all boxes. In the first checkbox replace (version of SAQ) with A



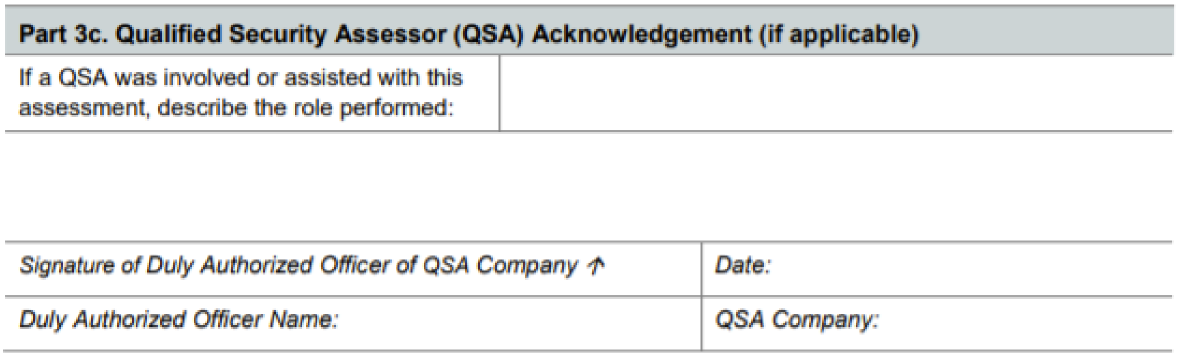
Part 3. PCI DSS Validation *(continued)*	
Part 3a. Acknowledgement of Status (continued)	
☐	No evidence of full track data[1], CAV2, CVC2, CID, or CVV2 data[2], or PIN data[3] storage after transaction authorization was found on ANY system reviewed during this assessment.
☐	ASV scans are being completed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

Check both boxes. Keep (ASV Name) blank if there is no scan.



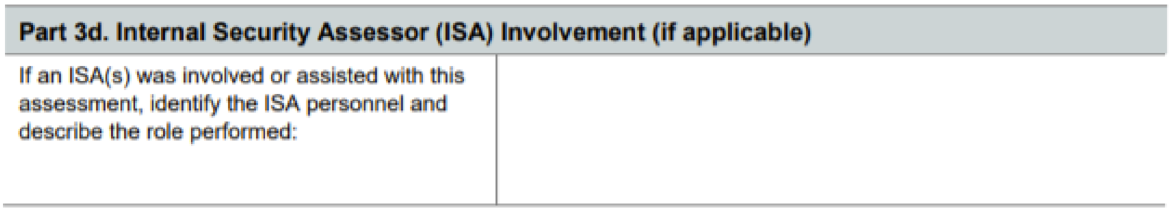
Part 3b. Merchant Attestation	
Signature of Merchant Executive Officer ↑	*Date:*
Merchant Executive Officer Name:	*Title:*

Physical or digital signature is acceptable.

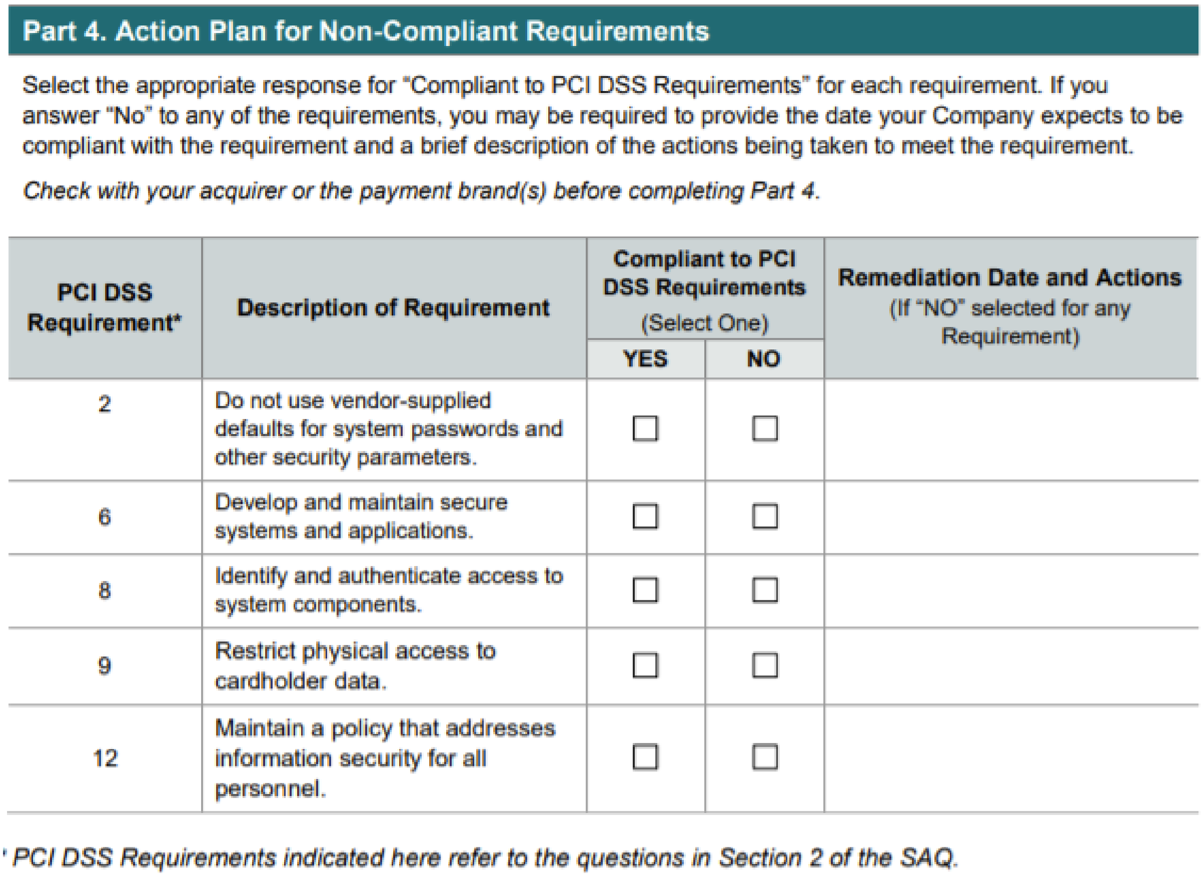


Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)	
If a QSA was involved or assisted with this assessment, describe the role performed:	
Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

Align to Part1b. If applicable, can be found here:
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors



Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)	
If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	



Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement. If you answer "No" to any of the requirements, you 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 "NO" selected for any Requirement)
		YES	NO	
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	□	□	
6	Develop and maintain secure systems and applications.	□	□	
8	Identify and authenticate access to system components.	□	□	
9	Restrict physical access to cardholder data.	□	□	
12	Maintain a policy that addresses information security for all personnel.	□	□	

' PCI DSS Requirements indicated here refer to the questions in Section 2 of the SAQ.

This part is used when client selected 'NO' in Section 2. However, we do not accept any 'No' situation, so if client selected NO, we should suggest the client take necessary actions to meet with the security standards