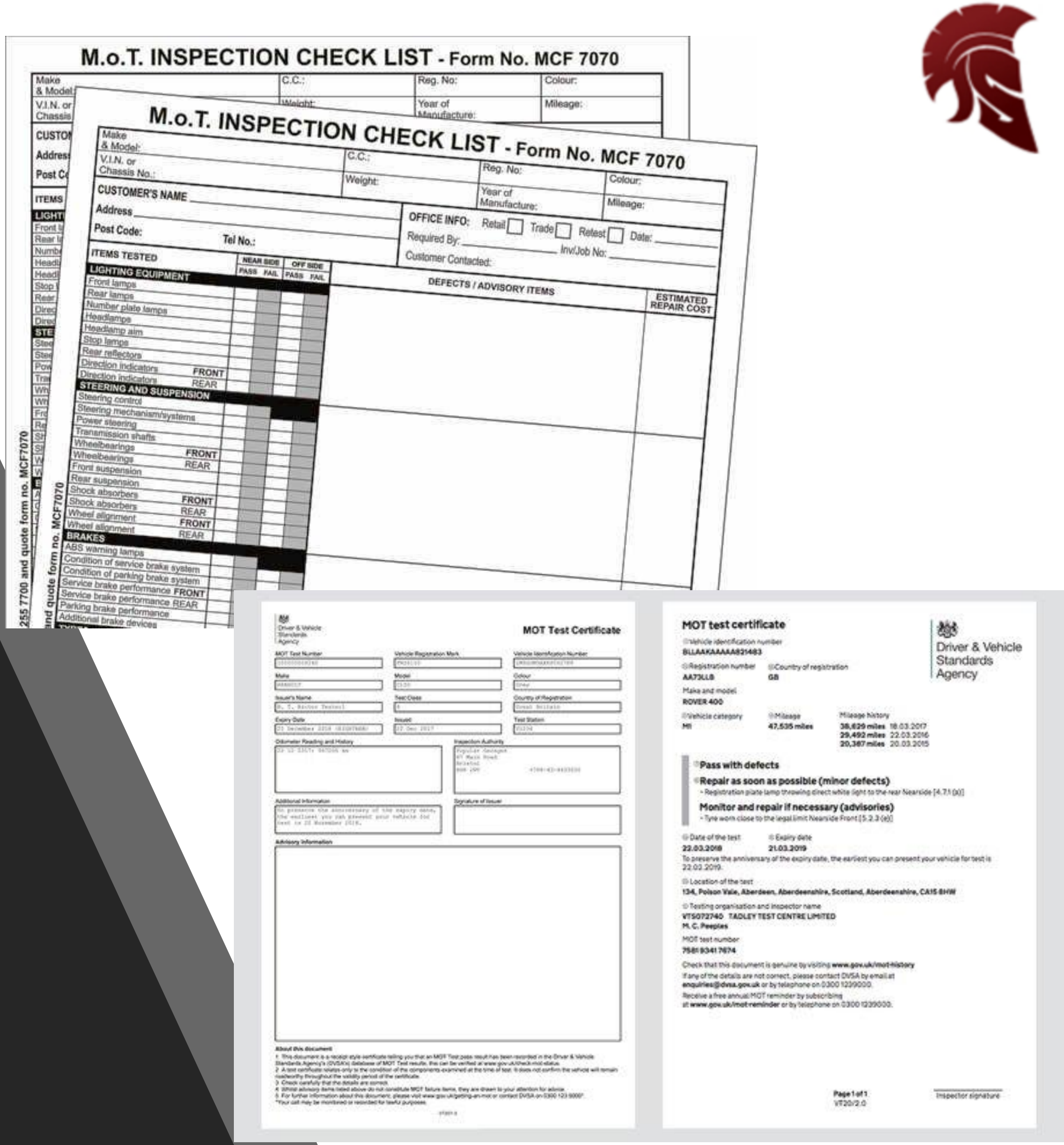
Safely Navigating PCI DSS Validation for the SMB Merchant

Understanding how to submit your annual compliance status

INFORMATION SECURITY
CENTURION

Understanding PCI DSS

- Applicability
- Annually Merchants are required to submit their status of PCI DSS compliance to their Acquiring Bank.
- Assessment:
  - Report on Compliance (RoC).
  - Self-Assessment Questionnaires (SAQ).
- Validation:
  - Attestation of Compliance (AoC).



M.o.T. INSPECTION CHECK LIST - Form No. MCF 7070

Make & Model:	C.C.:	Reg. No:	Colour:
V.I.N. or Chassis No.:	Weight:	Year of Manufacture:	Mileage:

CUSTOMER'S NAME

Address

Post Code: Tel No.:

OFFICE INFO: Retail □ Trade □ Retest □ Date:

Required By: Inv/Job No:

Customer Contacted:

ITEMS TESTED	NEAR SIDE PASS	NEAR SIDE FAIL	OFF SIDE PASS	OFF SIDE FAIL	DEFECTS / ADVISORY ITEMS	ESTIMATED REPAIR COST
LIGHTING EQUIPMENT						
Front lamps						
Rear lamps						
Number plate lamps						
Headlamps						
Headlamp aim						
Stop lamps						
Rear reflectors						
Direction indicators FRONT						
Direction indicators REAR						
STEERING AND SUSPENSION						
Steering control						
Steering mechanism/systems						
Power steering						
Transmission shafts						
Wheelbearings FRONT						
Wheelbearings REAR						
Front suspension						
Rear suspension						
Shock absorbers FRONT						
Shock absorbers REAR						
Wheel alignment FRONT						
Wheel alignment REAR						
BRAKES						
ABS warning lamps						
Condition of service brake system						
Condition of parking brake system						
Service brake performance FRONT						
Service brake performance REAR						
Parking brake performance						
Additional brake devices						

255 7700 and quote form no. MCF7070

Driver & Vehicle Standards Agency

MOT Test Certificate

MOT Test Number	Vehicle Registration Mark	Vehicle Identification Number
[illegible]	[illegible]	[illegible]
Make	Model	Colour
[illegible]	[illegible]	[illegible]
Issuer's Name	Test Class	Country of Registration
[illegible]	4	Great Britain
Expiry Date	Issued	Test Station
[illegible]	[illegible]	[illegible]

Odometer Reading and History

[illegible]

Inspection Authority

[illegible]

Additional Information

To preserve the anniversary of the expiry date, the earliest you can present your vehicle for test is 22 November 2018.

Signature of Issuer

Advisory Information

About this document

1. This document is a receipt style certificate telling you that an MOT Test pass result has been recorded in the Driver & Vehicle Standards Agency's (DVSA's) database of MOT Test results, this can be verified at www.gov.uk/check-mot-status.
2. A test certificate relates only to the condition of the components examined at the time of test. It does not confirm the vehicle will remain roadworthy throughout the validity period of the certificate.
3. Check carefully that the details are correct.
4. Whilst advisory items listed above do not constitute MOT failure items, they are drawn to your attention for advice.
5. For further information about this document, please visit www.gov.uk/getting-an-mot or contact DVSA on 0300 123 9000*.

*Your call may be monitored or recorded for lawful purposes.

MOT test certificate

Driver & Vehicle Standards Agency

Vehicle identification number
BLLAAKAAAAA831483

Registration number
AA73LLB

Country of registration
GB

Make and model
ROVER 400

Vehicle category
M1

Mileage
47,535 miles

Mileage history
38,629 miles 18.03.2017
29,492 miles 22.03.2016
20,367 miles 20.03.2015

Pass with defects

Repair as soon as possible (minor defects)
- Registration plate lamp throwing direct white light to the rear Nearside [4.7.1 (a)]

Monitor and repair if necessary (advisories)
- Tyre worn close to the legal limit Nearside Front [5.2.3 (e)]

Date of the test
22.03.2018

Expiry date
21.03.2019

To preserve the anniversary of the expiry date, the earliest you can present your vehicle for test is 22.02.2019.

Location of the test
134, Polson Vale, Aberdeen, Aberdeenshire, Scotland, Aberdeenshire, CA15 8HW

Testing organisation and inspector name
VTS072740 TADLEY TEST CENTRE LIMITED
M. C. Peeples

MOT test number
7581 9341 7674

Check that this document is genuine by visiting **www.gov.uk/mot-history**

If any of the details are not correct, please contact DVSA by email at **enquiries@dvsa.gov.uk** or by telephone on 0300 1239000.

Receive a free annual MOT reminder by subscribing at **www.gov.uk/mot-reminder** or by telephone on 0300 1239000.

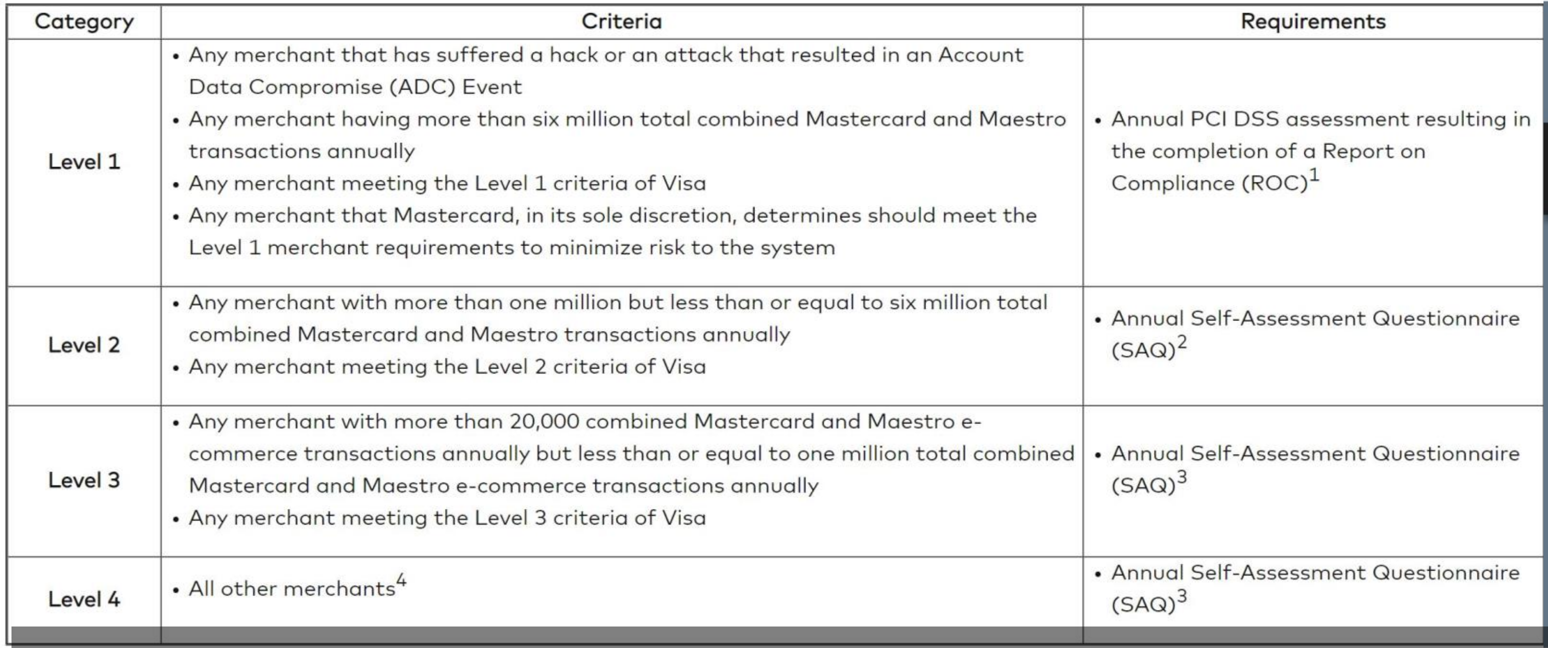
Page 1 of 1
VT20/2.0

Inspector signature

Risk-Based Validation

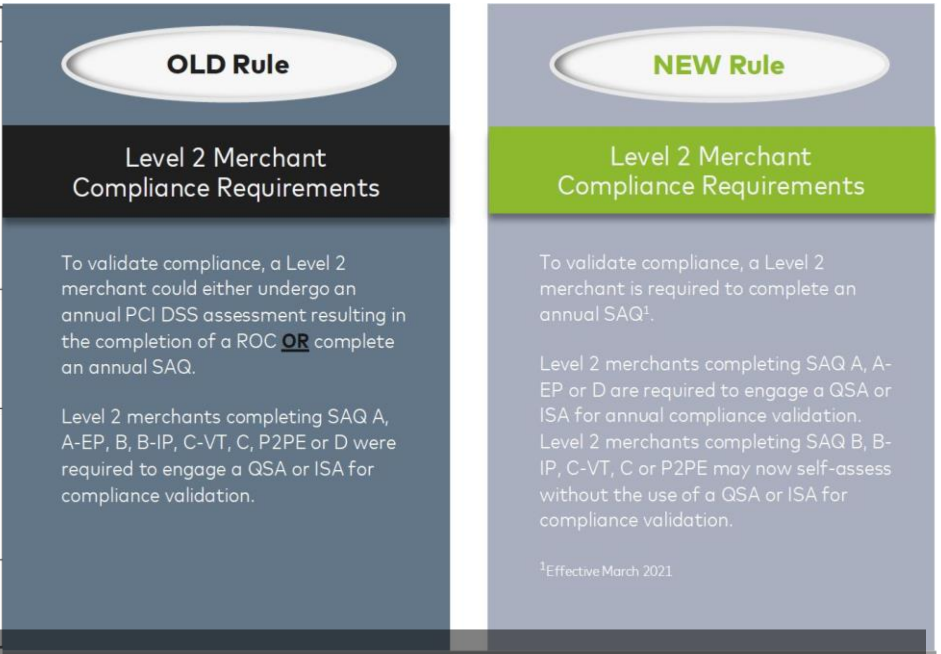
- Validation requirements are driven by:
  - Volume of payment card transactions per annum.
  - Methods of taking card payments.
- High-Volume or High-Risk payment operations:
  - Assessments conducted by a PCI Qualified Security Assessor.
    - RoC & AoC.
- Lower-risk or Lower-Risk payment operations:
  - SAQ & AoC.

PCI DSS Compliance Validation:Mastercard



Category	Criteria	Requirements
Level 1	• Any merchant that has suffered a hack or an attack that resulted in an Account Data Compromise (ADC) Event • Any merchant having more than six million total combined Mastercard and Maestro transactions annually • Any merchant meeting the Level 1 criteria of Visa • Any merchant that Mastercard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system	• Annual PCI DSS assessment resulting in the completion of a Report on Compliance (ROC)[1]
Level 2	• Any merchant with more than one million but less than or equal to six million total combined Mastercard and Maestro transactions annually • Any merchant meeting the Level 2 criteria of Visa	• Annual Self-Assessment Questionnaire (SAQ)[2]
Level 3	• Any merchant with more than 20,000 combined Mastercard and Maestro e-commerce transactions annually but less than or equal to one million total combined Mastercard and Maestro e-commerce transactions annually • Any merchant meeting the Level 3 criteria of Visa	• Annual Self-Assessment Questionnaire (SAQ)[3]
Level 4	• All other merchants[4]	• Annual Self-Assessment Questionnaire (SAQ)[3]

Current



OLD Rule

Level 2 Merchant
Compliance Requirements

To validate compliance, a Level 2 merchant could either undergo an annual PCI DSS assessment resulting in the completion of a ROC **OR** complete an annual SAQ.

Level 2 merchants completing SAQ A, A-EP, B, B-IP, C-VT, C, P2PE or D were required to engage a QSA or ISA for compliance validation.

NEW Rule

Level 2 Merchant
Compliance Requirements

To validate compliance, a Level 2 merchant is required to complete an annual SAQ[1].

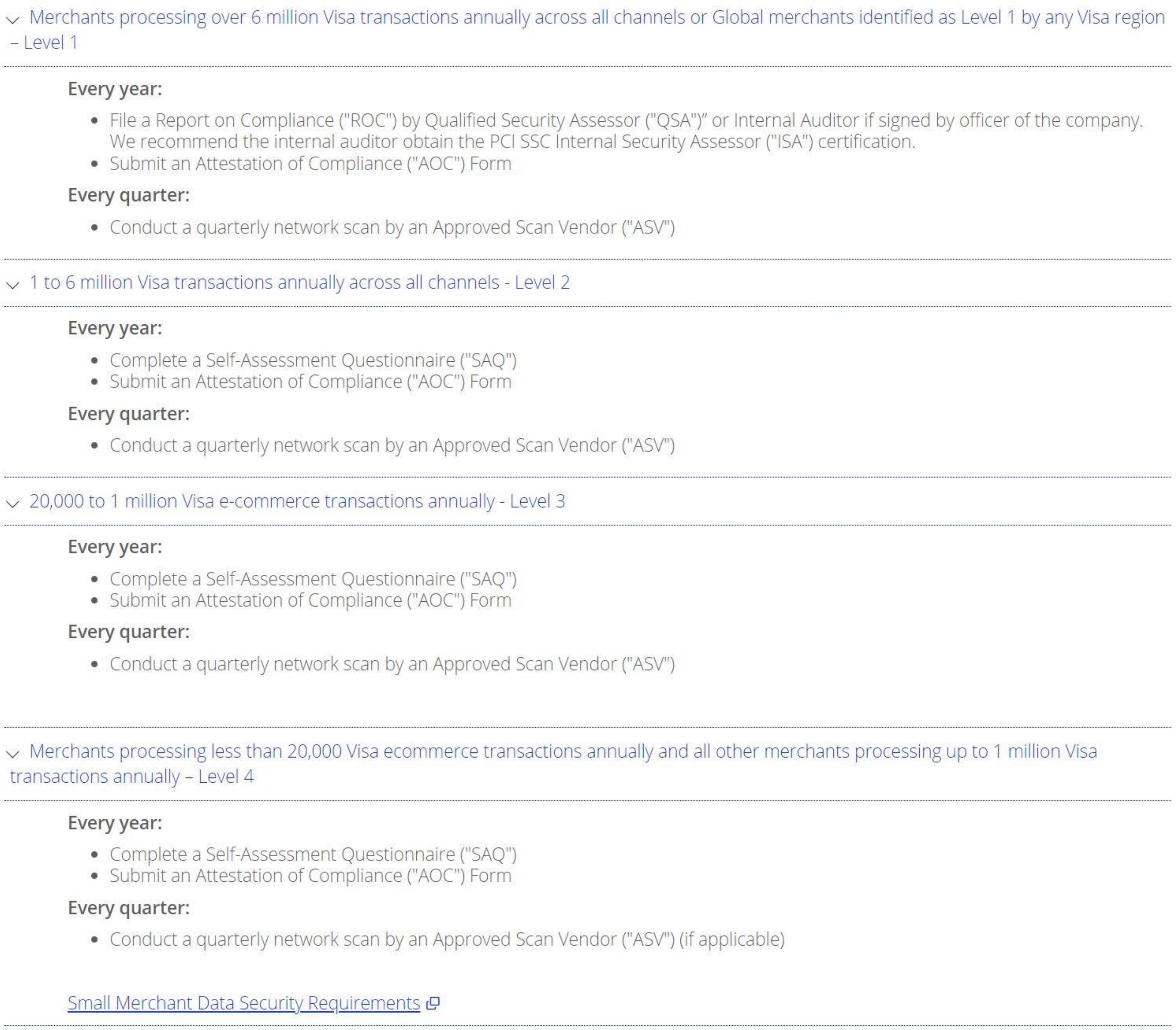
Level 2 merchants completing SAQ A, A-EP or D are required to engage a QSA or ISA for annual compliance validation. Level 2 merchants completing SAQ B, B-IP, C-VT, C or P2PE may now self-assess without the use of a QSA or ISA for compliance validation.

[1]Effective March 2021

Changed – Level 2 Merchants

PCI DSS Compliance Validation: VISA

- *Take the time to see that you've met all requirements of the PCI Data Security Standard (DSS).*
- *It's the best way to confirm cardholder data is being safely handled and to expose any weaknesses that need to be addressed.*
- *Your total Visa transaction volume over a 12-month period determines your merchant level and the necessary requirements for validation.*



Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region – Level 1

Every year:

- File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")" or Internal Auditor if signed by officer of the company. We recommend the internal auditor obtain the PCI SSC Internal Security Assessor ("ISA") certification.
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

1 to 6 million Visa transactions annually across all channels - Level 2

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

20,000 to 1 million Visa e-commerce transactions annually - Level 3

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV")

Merchants processing less than 20,000 Visa ecommerce transactions annually and all other merchants processing up to 1 million Visa transactions annually – Level 4

Every year:

- Complete a Self-Assessment Questionnaire ("SAQ")
- Submit an Attestation of Compliance ("AOC") Form

Every quarter:

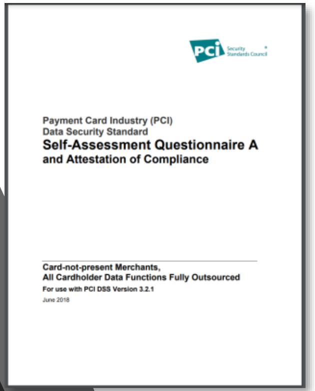
- Conduct a quarterly network scan by an Approved Scan Vendor ("ASV") (if applicable)

Small Merchant Data Security Requirements

Types of SAQ

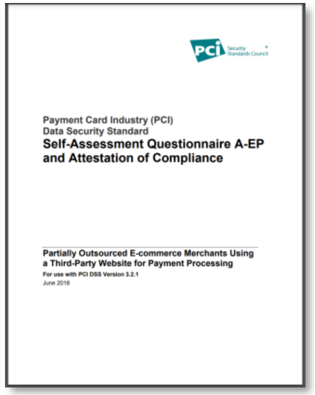
1. SAQ A
2. SAQ A-EP
3. SAQ B
4. SAQ B-IP
5. SAQ C-VT
6. SAQ C
7. SAQ P2PE
8. SAQ D Merchant
9. SAQ D Service Provider

Source: https://www.pcisecuritystandards.org/document_library



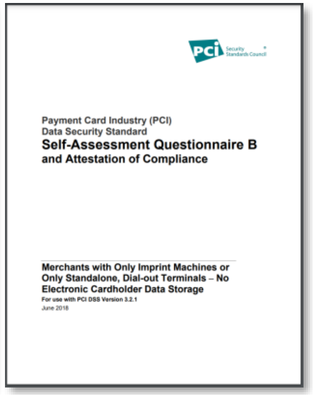
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A
and Attestation of Compliance

Card-not-present Merchants,
All Cardholder Data Functions Fully Outsourced
For use with PCI DSS Version 3.2.1
June 2018



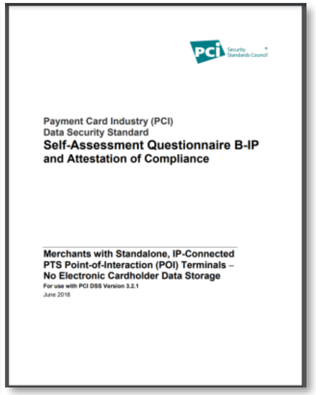
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire A-EP
and Attestation of Compliance

Partially Outsourced E-commerce Merchants Using
a Third-Party Website for Payment Processing
For use with PCI DSS Version 3.2.1
June 2018



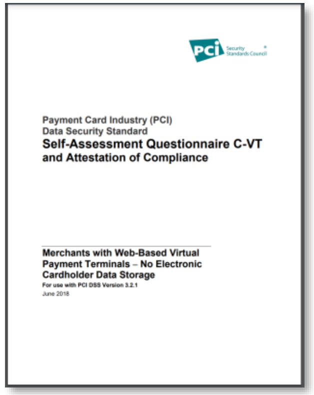
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire B
and Attestation of Compliance

Merchants with Only Imprint Machines or
Only Standalone, Dial-out Terminals – No
Electronic Cardholder Data Storage
For use with PCI DSS Version 3.2.1
June 2018



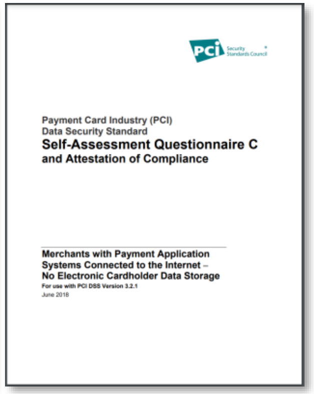
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire B-IP
and Attestation of Compliance

Merchants with Standalone, IP-Connected
PTS Point-of-Interaction (POI) Terminals –
No Electronic Cardholder Data Storage
For use with PCI DSS Version 3.2.1
June 2018



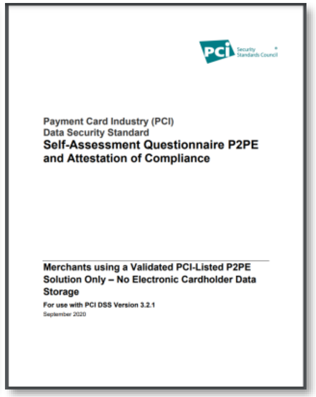
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire C-VT
and Attestation of Compliance

Merchants with Web-Based Virtual
Payment Terminals – No Electronic
Cardholder Data Storage
For use with PCI DSS Version 3.2.1
June 2018



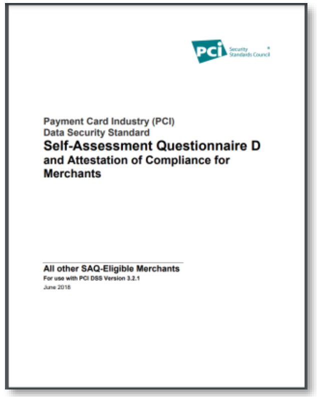
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire C
and Attestation of Compliance

Merchants with Payment Application
Systems Connected to the Internet –
No Electronic Cardholder Data Storage
For use with PCI DSS Version 3.2.1
June 2018



Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire P2PE
and Attestation of Compliance

Merchants using a Validated PCI-Listed P2PE
Solution Only – No Electronic Cardholder Data
Storage
For use with PCI DSS Version 3.2.1
September 2020



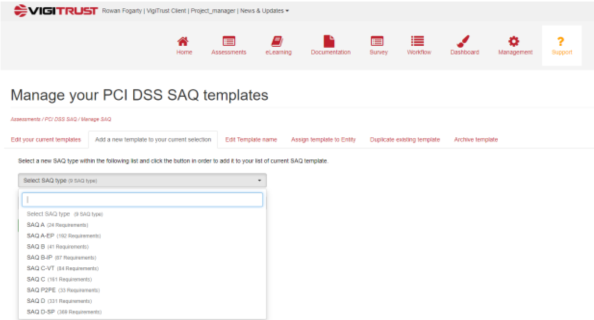
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire D
and Attestation of Compliance for
Merchants

All other SAQ-Eligible Merchants
For use with PCI DSS Version 3.2.1
June 2018

SAQ Completion for Merchants

- On VigiOne you create a template for any one of the 8 types of SAQ Merchant and the SAQ Service Provider
- Each SAQ generates an associated AOC

VIGIONE


VIGITRUST
Rowan Fogarty | VigiTrust Client | Project_manager | News & Updates
Home
Assessments
eLearning
Documentation
Survey
Workflow
Dashboard
Management
Support
Edit your current templates
Add a new template to your current selection
Edit Template name
Assign template to Entity
Duplicate existing template
Archive template

Manage your PCI DSS SAQ templates

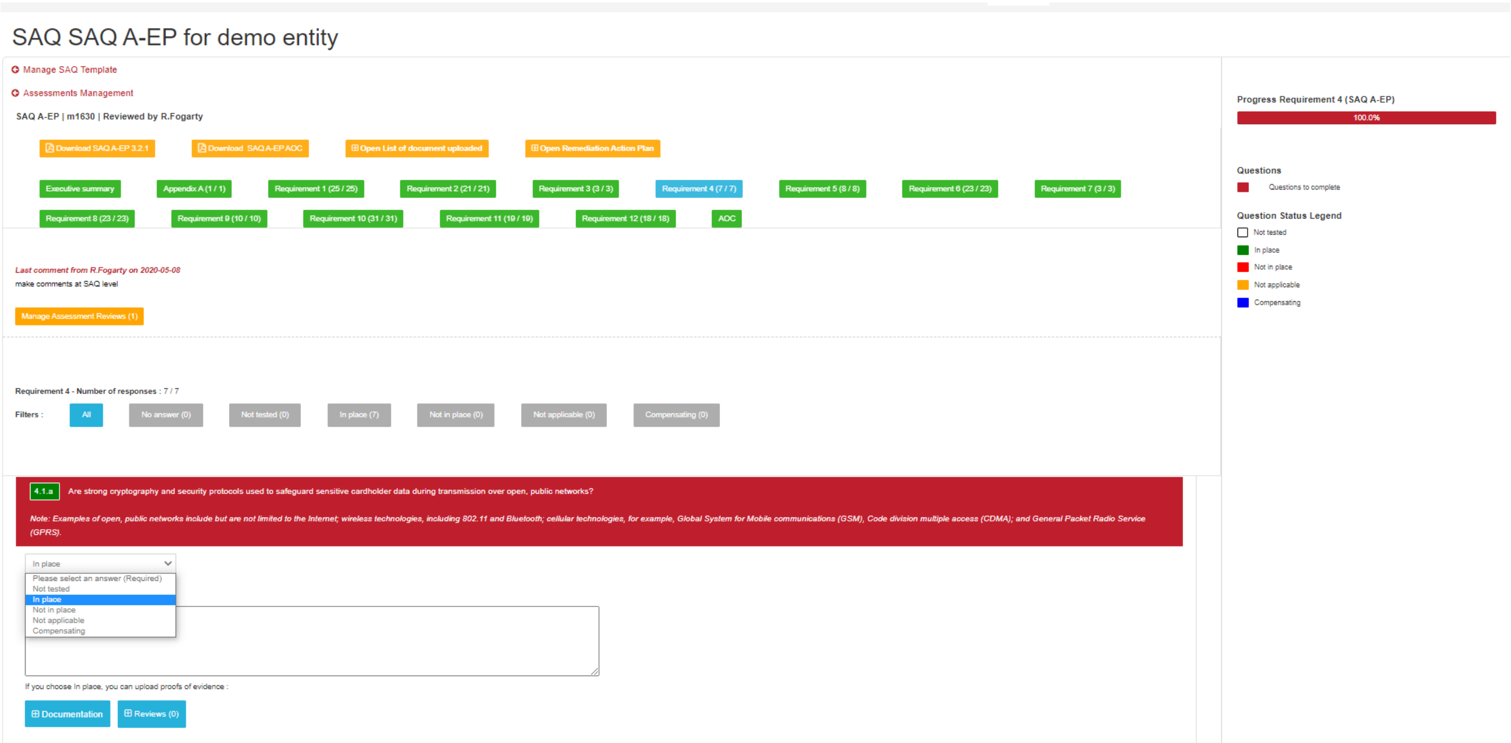
Assessments / PCI DSS SAQ / Manage SAQ

Select a new SAQ type within the following list and click the button in order to add it to your list of current SAQ template.

Select SAQ type (9 SAQ type)

Select SAQ type (9 SAQ type)
SAQ A (24 Requirements)
SAQ A-EP (192 Requirements)
SAQ B (41 Requirements)
SAQ B-IP (87 Requirements)
SAQ C-VT (84 Requirements)
SAQ C (161 Requirements)
SAQ P2PE (33 Requirements)
SAQ D (331 Requirements)
SAQ D-SP (369 Requirements)

VigiOne's SAQ tool allows you complete an SAQ



SAQ SAQ A-EP for demo entity

SAQ A-EP | m1630 | Reviewed by R.Fogarty

Last comment from R.Fogarty on 2020-05-08

make comments at SAQ level

Requirement 4 - Number of responses : 7 / 7

Filters :

4.1.a Are strong cryptography and security protocols used to safeguard sensitive cardholder data during transmission over open, public networks?

Note: Examples of open, public networks include but are not limited to the Internet; wireless technologies, including 802.11 and Bluetooth; cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA); and General Packet Radio Service (GPRS).

In place

If you choose In place, you can upload proofs of evidence :

Progress Requirement 4 (SAQ A-EP)

100.0%

Questions

🟥 Questions to complete

Question Status Legend

□ Not tested

🟩 In place

🟥 Not in place

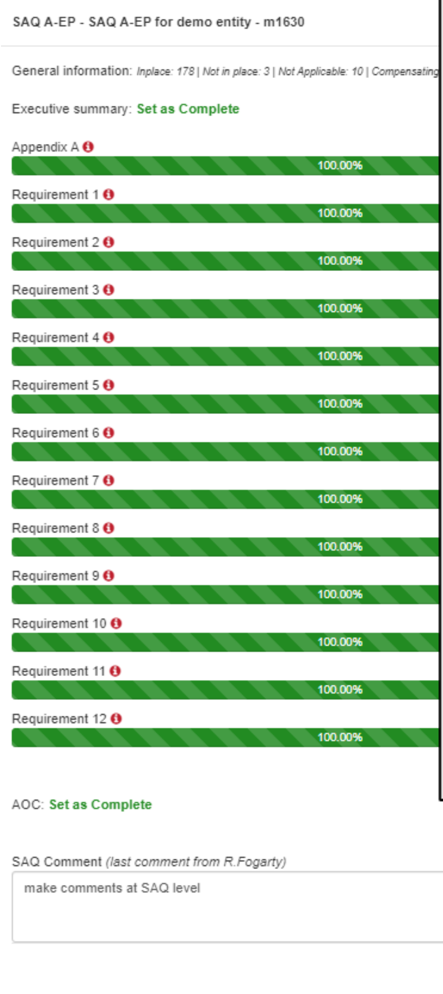
🟧 Not applicable

🟦 Compensating

VIGIONE

VigiOne’s SAQ Tool tracks completion & produces documentation

- Enables completion
- Evidence Upload
- Review by ISA or QSA
- Provides a status report
- Download and print documentation



SAQ A-EP - SAQ A-EP for demo entity - m1630

General information: *Inplace: 178 | Not in place: 3 | Not Applicable: 10 | Compensating*

Executive summary: Set as Complete

Appendix A 100.00%

Requirement 1 100.00%

Requirement 2 100.00%

Requirement 3 100.00%

Requirement 4 100.00%

Requirement 5 100.00%

Requirement 6 100.00%

Requirement 7 100.00%

Requirement 8 100.00%

Requirement 9 100.00%

Requirement 10 100.00%

Requirement 11 100.00%

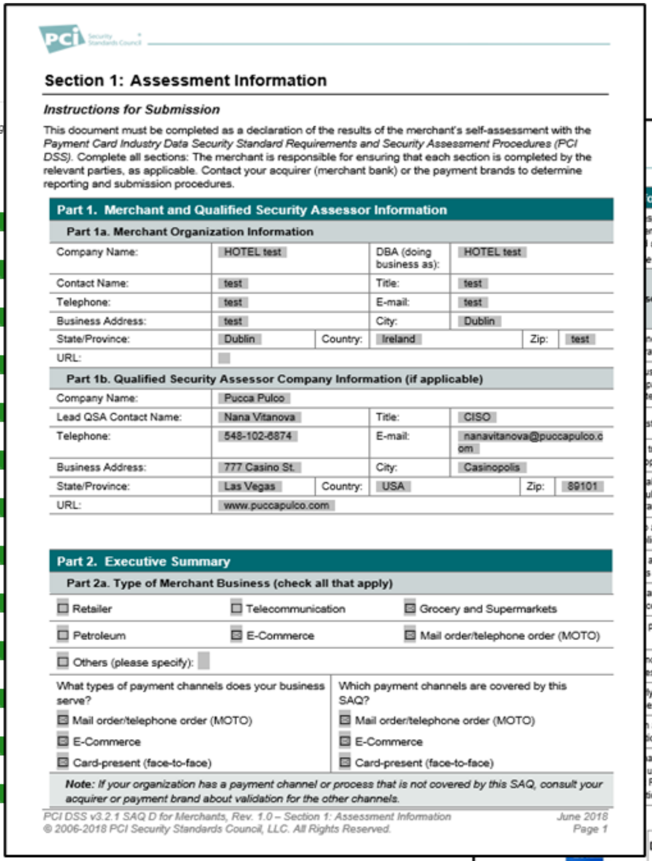
Requirement 12 100.00%

AOC: Set as Complete

SAQ Comment *(last comment from R.Fogarty)*

make comments at SAQ level

Access SAQ
Close



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 your acquirer (merchant bank) or the payment brands to determine reporting and submission procedures.

Part 1. Merchant and Qualified Security Assessor Information

Part 1a. Merchant Organization Information

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

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

Company Name:	Pucca Pulco				
Lead QSA Contact Name:	Nana Vitanova		Title:	CISO	
Telephone:	548-102-6874		E-mail:	nanavitanova@puccapulco.com	
Business Address:	777 Casino St.		City:	Casinopolis	
State/Province:	Las Vegas	Country:	USA	Zip:	89101
URL:	www.puccapulco.com				

Part 2. Executive Summary

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

□ Retailer □ Telecommunication ☒ Grocery and Supermarkets

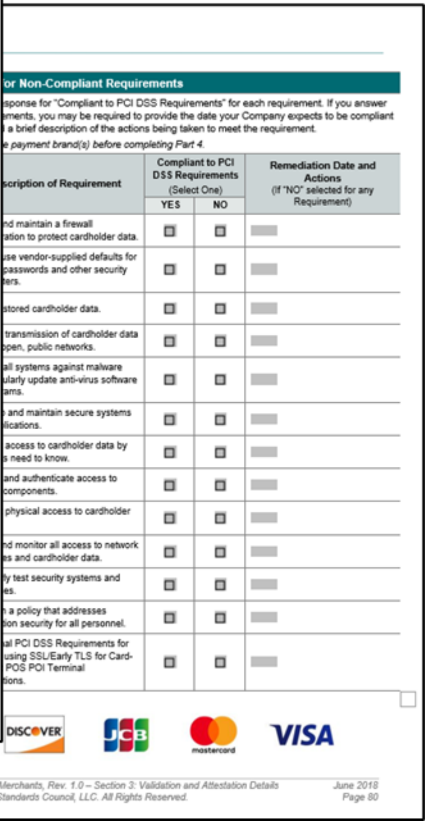
□ Petroleum ☒ E-Commerce ☒ Mail order/telephone order (MOTO)

□ Others (please specify):

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

PCI DSS v3.2.1 SAQ D for Merchants, Rev. 1.0 – Section 1: Assessment Information *June 2018*
© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved. *Page 1*



or Non-Compliant Requirements

sponse for "Compliant to PCI DSS Requirements" for each requirement. If you answer ements, you may be required to provide the date your Company expects to be compliant a brief description of the actions being taken to meet the requirement.

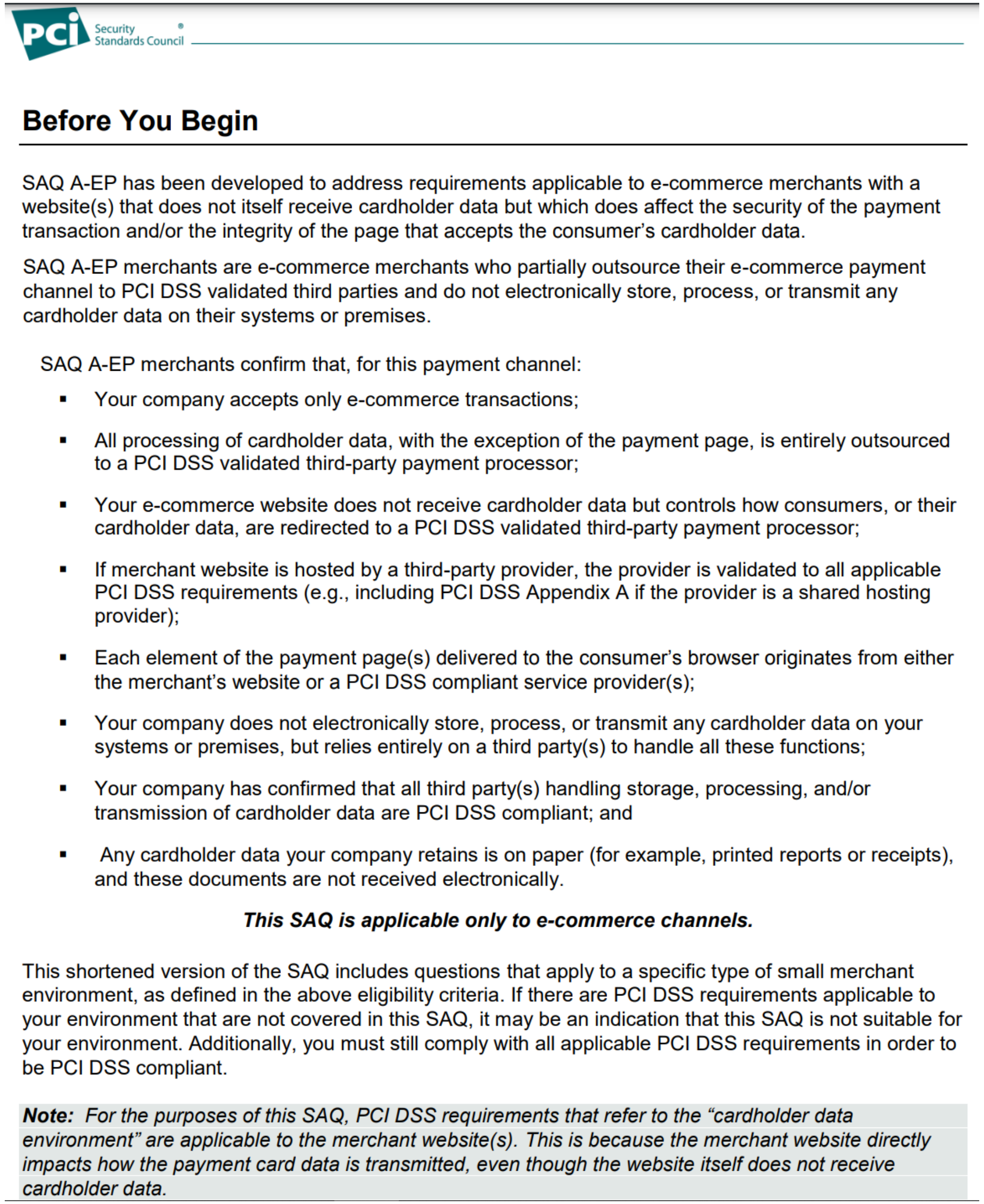
e payment brand(s) before completing Part 4.

scription of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
	YES	NO	
nd maintain a firewall ration to protect cardholder data.	□	□	
use vendor-supplied defaults for passwords and other security ters.	□	□	
stored cardholder data.	□	□	
transmission of cardholder data open, public networks.	□	□	
all systems against malware ularly update anti-virus software ams.	□	□	
and maintain secure systems lications.	□	□	
access to cardholder data by s need to know.	□	□	
and authenticate access to components.	□	□	
physical access to cardholder	□	□	
nd monitor all access to network es and cardholder data.	□	□	
ly test security systems and es.	□	□	
a policy that addresses ion security for all personnel.	□	□	
al PCI DSS Requirements for using SSL/Early TLS for Card-POS POI Terminal tions.	□	□	

PCI DSS v3.2.1 SAQ D for Merchants, Rev. 1.0 – Section 3: Validation and Attestation Details *June 2018*
© 2006-2018 PCI Security Standards Council, LLC. All Rights Reserved. *Page 80*

Which SAQ is right for you?

- **Each SAQ has a differing number of applicable controls:**
  - SAQ A – Fully outsourced.
    - Circa 24 security controls.
  - SAQ D – Fully in-house.
    - Circa 330 security controls.
- **Always ensure that you are meeting the SAQ Criteria.**
  - **Before You Begin**



PCI Security Standards Council

Before You Begin

SAQ A-EP has been developed to address requirements applicable to e-commerce merchants with a website(s) that does not itself receive cardholder data but which does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data.

SAQ A-EP merchants are e-commerce merchants who partially outsource their e-commerce payment channel to PCI DSS validated third parties and do not electronically store, process, or transmit any cardholder data on their systems or premises.

SAQ A-EP merchants confirm that, for this payment channel:

- Your company accepts only e-commerce transactions;
- All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor;
- Your e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor;
- If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider);
- Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s);
- 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.

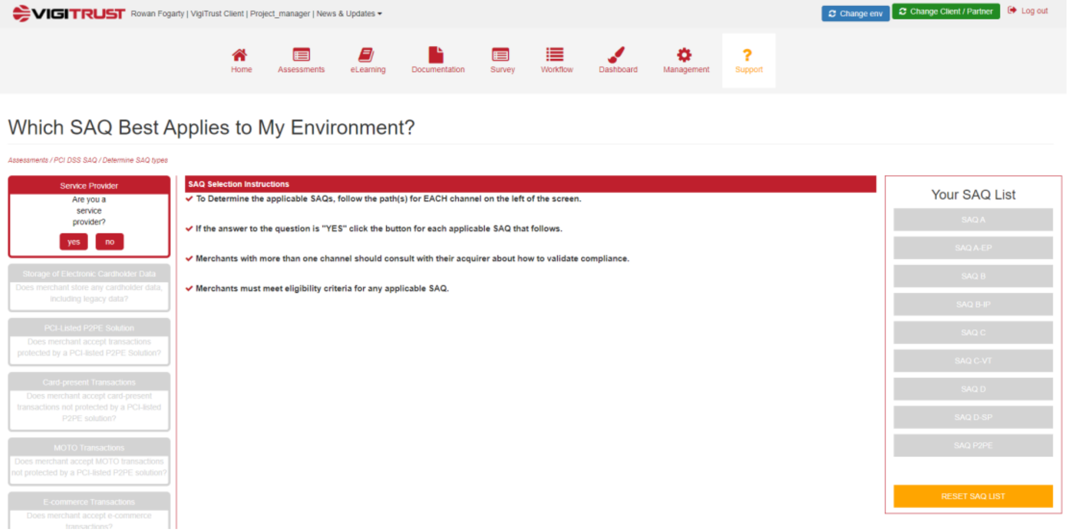
This SAQ is applicable only to e-commerce channels.

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 the purposes of this SAQ, PCI DSS requirements that refer to the "cardholder data environment" are applicable to the merchant website(s). This is because the merchant website directly impacts how the payment card data is transmitted, even though the website itself does not receive cardholder data.*

Which SAQ Guide Tool.

- Based on the guidelines from the PCI SSC the tool enables a merchant to determine which SAQs may apply



Which SAQ Best Applies to My Environment?

Assessments / PCI DSS SAQ / Determine SAQ types

Service Provider

Are you a service provider?

Storage of Electronic Cardholder Data

Does merchant store any cardholder data, including legacy data?

PCI-Listed P2PE Solution

Does merchant accept transactions protected by a PCI-listed P2PE Solution?

Card-present Transactions

Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution?

MOTO Transactions

Does merchant accept MOTO transactions not protected by a PCI-listed P2PE solution?

E-commerce Transactions

Does merchant accept e-commerce transactions?

SAQ Selection Instructions

- ✓ To Determine the applicable SAQs, follow the path(s) for EACH channel on the left of the screen.
- ✓ If the answer to the question is "YES" click the button for each applicable SAQ that follows.
- ✓ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✓ Merchants must meet eligibility criteria for any applicable SAQ.

Your SAQ List