Which Self-Assessment Is Right For You?

PCI Compliance & Sustainability

Payment Card Assessments, LLC

# PCI Self-Assessment Eligibility Guide

JULY 2023

PAYMENTCARDASSESSMENTS.COM

# Table of Contents

# Who This SAQ Eligibility Guide is For

This Guide is to help merchants that are NOT level 1 merchants determine which PCI Self-Assessment Questionnaire (SAQ) is applicable to their cardholder data environment.

# Disclaimer: (because we need to have one)

The intent of this guide is to help merchants determine which SAQ they should use for their annual PCI self-assessment.

This guide is NOT for Level 1 merchants.

PCI Self-Assessments can only be used by the following:

- Level 4 merchants
- Level 3 merchants
- Level 2 merchants

Not sure of your merchant level? Contact your acquirer.

**NOTE: Eligibility Criteria is based on PCI DSS v4.0 for all SAQs in this guide.**

# Welcome

## Which SAQ is right for you?

PCI Compliance is complicated. And it doesn't matter what level merchant you are. You're in business to do business, make money, and generate a profit. You're not in business to make sense of PCI Compliance.

But aren't you glad we're in business to help you make sense of PCI DSS Compliance?

We want you to be able to deliver your attestation of compliance based on the SAQ that's right for your organization, as painlessly as possible.

So let’s get started, shall we?

**Here's to your success,**

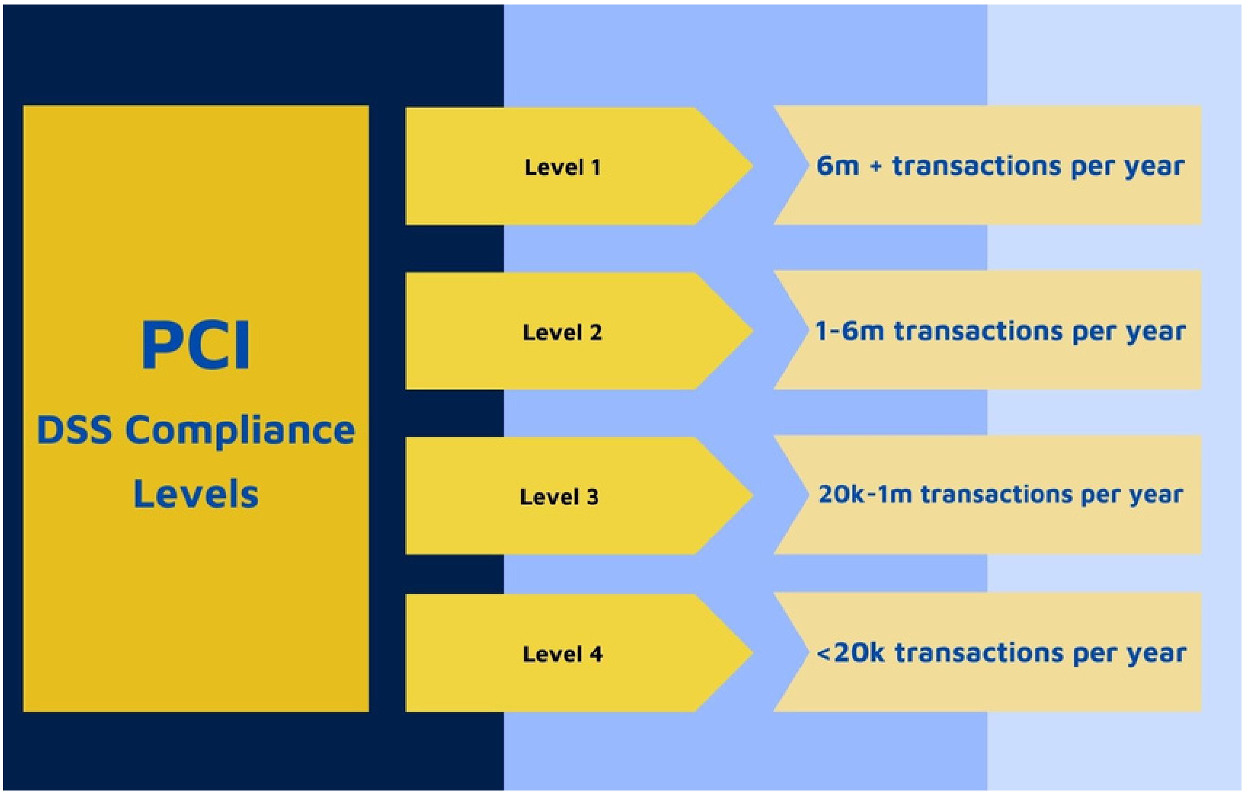
Peggy & Lisa

MERCHANT LEVELS

# Merchant Levels

WHAT ARE THEY?

If you're not sure of your transaction volume, contact your acquirer!


PCI
DSS Compliance Levels
Level 1
6m + transactions per year
Level 2
1-6m transactions per year
Level 3
20k-1m transactions per year
Level 4
<20k transactions per year

# 5 Steps to Complete A PCI DSS Self-Assessment

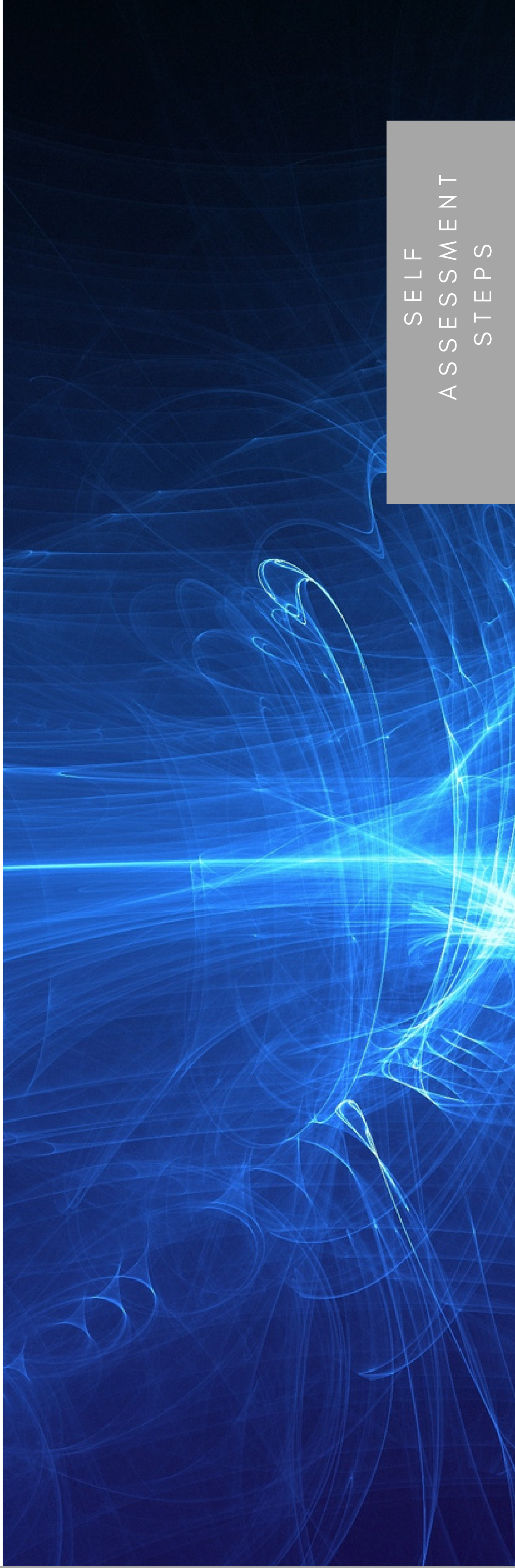
Merchants with less than 6 million transactions a year are eligible to complete the applicable SAQ for their annual attestation of compliance.

## 5 Steps:

- Confirm you're completing the correct SAQ.
- Complete an accurate scope assessment prior to completing your SAQ
- Assess your environment for PCI DSS compliance
  - Collect evidence
  - Interview personnel
  - Ensure all policies, standards, and processes are current
- Complete all sections of your SAQ
- Submit your SAQ, AoC, and ASV scans (as applicable) to your acquirer or requesting organziation

If completing your Self Assessment is confusing, email us at support@paymentcardassessments.com

## We Can Help!



SELF ASSESSMENT STEPS

# Self-Assessment Elegibility Requirements

There are as many Self-Assessment Questionnaires as there are ways to accept credit cards for payment of goods and services.

The rest of this document breaks down the eligibility requirements for each SAQ.

**Remember, if you're a Level 1 merchant, this guide isn't for you. You need our Report on Compliance Planner and our Consolidated Interview and Observation Schedule.**

# SAQ A Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| The merchant accepts only card-not-present (e-commerce or mail/telephone-order) transaction. | | |
| All processing of account data is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor. | | |
| The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions. | | |
| The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and confirmed that TPSP(s) are PCI DSS compliant for the services being used by the merchant. | | |
| Any account data the merchant might retain 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)/form(s) delivered to the customer’s browser originate only and directly from a PCI DSS compliant TPSP/payment processor. | | |

# SAQ A-EP Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| The merchant accepts only e-commerce transactions. | | |
| All processing of account data, with the exception of the payment page, is entirely outsourced to a PCI DSS compliant third-party service provider (TPSP)/payment processor. | | |
| The merchant's e-commerce website does not receive account data but controls how customers, or their account data, are redirected to a PCI DSS compliant TPSP/payment processor. | | |
| If merchant website is hosted by a TPSP, the TPSP is compliant with all applicable PCI DSS requirements (for example, including PCI DSS Appendix A if the TPSP is a multi-tenant hosting provider). | | |
| Each element of the payment page(s) delivered to the customer's browser originates from either the merchant's website or a PCI DSS compliant TPSP. | | |
| The merchant does not electronically store, process, or transmit any account data on merchant systems or premises, but relies entirely on a TPSP(s) to handle all these functions. | | |
| The merchant has reviewed the PCI DSS Attestation of Compliance form(s) for its TPSP(s) and has confirmed that TPSP(s) are PCI DSS compliant for the services used by the merchant. | | |
| Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. | | |

# SAQ B Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| The merchant uses only an imprint machine and/or uses only standalone, dial-out terminals (connected via a phone line the merchant processor) to take customers' payment card information. | | |
| The standalone, dial-out terminals are not connected to any other systems within the merchant environment. | | |
| The standalone, dial-out terminals are not connected to the Internet. | | |
| The merchant does not store account data in electronic format. | | |
| Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. | | |

# SAQ C Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| The merchant has a payment application system and an Internet connection on the same device and/or same local area network (LAN). | | |
| The payment application system is not connected to any other system within the merchant environment. | | |
| The physical location of the POS environment is not connected to other premises or locations, and any LAN is for a single location only. | | |
| Merchant does not store account data in electronic format. | | |
| Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. | | |

# SAQ C-VT Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| The only payment processing is via a virtual payment terminal accessed by an Internet-connected web browser. | | |
| The virtual payment terminal solution is provided and hosted by a PCI DSS validated third-party service provider. | | |
| The PCI DSS-compliant virtual payment terminal solution is only accessed via a computing device that is isolated in a single location and is not connected to other locations or systems. | | |
| The computing device does not have software installed that causes account data to be stored (for example, there is no software for batch processing or store-and-forward). | | |
| The computing device does not have any attached hardware devices that are used to capture or store account data (for example, there are no card readers attached). | | |
| The merchant does not otherwise receive, transmit, or store account data electronically through any channels (for example, via an internal network or the Internet). | | |
| Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. | | |

# SAQ P2PE Eligibility Requirements

**Merchant certifies eligibility to complete this Self-Assessment Questionnaire because, for this payment (all responses must be YES)**

| Eligibility Criteria | Yes | No |
|---|---|---|
| All payment processing is via a validated PCI-listed P2PE solution (You must use a PCI listed P2PE solution) | | |
| The only systems in the merchant environment that store, process, or transmit account data are the payment terminals from a validated PCI-listed P2PE solution. | | |
| The merchant does not otherwise receive, transmit, or store account data electronically. | | |
| Any account data the merchant might retain is on paper (for example, printed reports or receipts), and these documents are not received electronically. | | |
| The merchant has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider. | | |

# SAQ D Eligibility Requirements

## Merchants

**If your organization does not meet the eligibility requirements for any of the previous Self-Assessments AND your organization is a Level 2, 3, or 4, then you will complete a SAQ D.**

## Service Providers

**Service Providers must complete a SAQ D for Service Providers**

# Assessment Best Practices

- Use Polaris PCA for your PCI Report on Compliance assessment and sustainability program.
  - Automated workflow
  - Built in knowledge base withPCI DSS authoritative sources
  - Best practices to help you save thousands of dollars in outside assessment fees
  - Best practices to help you save hundreds of hours in internal work effort
  - Learn more by emailing Payment Card Assessments at support@paymentcardassessments.com

- Use the PCA Scope Assessment Guide Book

- Use the PCA Consolidated Interview and Observation Schedule
  - Practice interviews with system administrators before they are interviewed by the QSA
  - Schedule and attend every interview & real time observation

- Create an effective communication plan using the templates provided in this planner

- Remember to assess documentation for annual reviews and current dates.

- Self collect evidence whenever and wherever possible.

- Coordinate and schedule all physical site visits at the beginning of the assessment phase
  - Ensure you've communicated expectations, requirements, and the real time observations the QSA will be making at each location

- Schedule a daily stand-up meeting with your QSA (meeting cadence may vary) to review
  - What requirements are "In place."
  - What requirements are "in progress."
  - What requirements are "not in place" and what the QSA needs to mark them "in place."

# Additional Resources

- PCI DSS: https://pcissc.org
- Download your applicable SAQ at https://pcissc.org

- Payment Card Assessments
    - Scope Assessment Guide
    - Workshops
    - Coaching
    - Gap assessments: email support@paymentcardassessments.com
    - Automate your next RoC or SAQ with Polaris PCA: email support@paymentcardassessments.com

# TAKE THE CHAOS OUT OF PCI COMPLIANCE

...

# AUTOMATE. EDUCATE. OPERATE.