

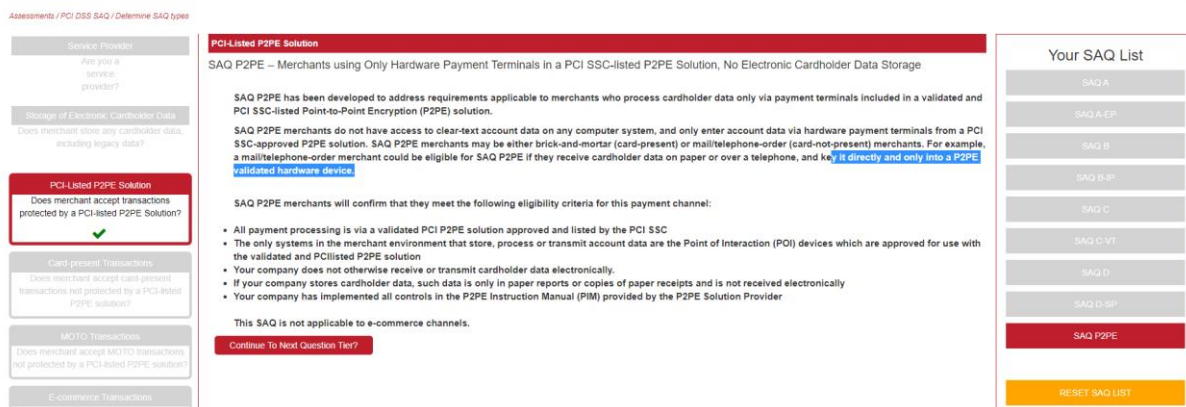
General:

VigiOne brings together all of VigiTrust's tools on to one platform in an integrated manner to allow you to manage compliance to multiple information security and data protection standards and regulations in one all-encompassing program.

1. Single view of compliance progress, evolution and KPI's
2. Flexible, robust & scalable GRC
3. Single repository of complicate activity and achievement

VigiOne as Merchant Compliance Platform (MCP) for PCI DSS

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 not protected by a PCI-listed P2PE solution?

PCI-Listed P2PE Solution
SAQ P2PE – Merchants using Only Hardware Payment Terminals in a PCI SSC-listed P2PE Solution, No Electronic Cardholder Data Storage

SAQ P2PE has been developed to address requirements applicable to merchants who process cardholder data only via payment terminals included in a validated and PCI SSC-listed Point-to-Point Encryption (P2PE) solution.

SAQ P2PE merchants do not have access to clear-text account data on any computer system, and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution. SAQ P2PE merchants may be either brick-and-mortar (card-present) or mail/telephone-order (card-not-present) merchants. For example, a mail/telephone-order merchant could be eligible for SAQ P2PE if they receive cardholder data on paper or over a telephone, and **key it directly and only into a P2PE validated hardware device**.

SAQ P2PE merchants will confirm that they meet the following eligibility criteria for this payment channel:

- All payment processing is via a validated PCI P2PE solution approved and listed by the PCI SSC
- The only systems in the merchant environment that store, process or transmit account data are the Point of Interaction (POI) devices which are approved for use with the validated and PCI-listed P2PE solution
- Your company does not otherwise receive or transmit cardholder data electronically.
- If your company stores cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically
- Your company has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider

This SAQ is not applicable to e-commerce channels.

Continue To Next Question Tier?

Your SAQ List

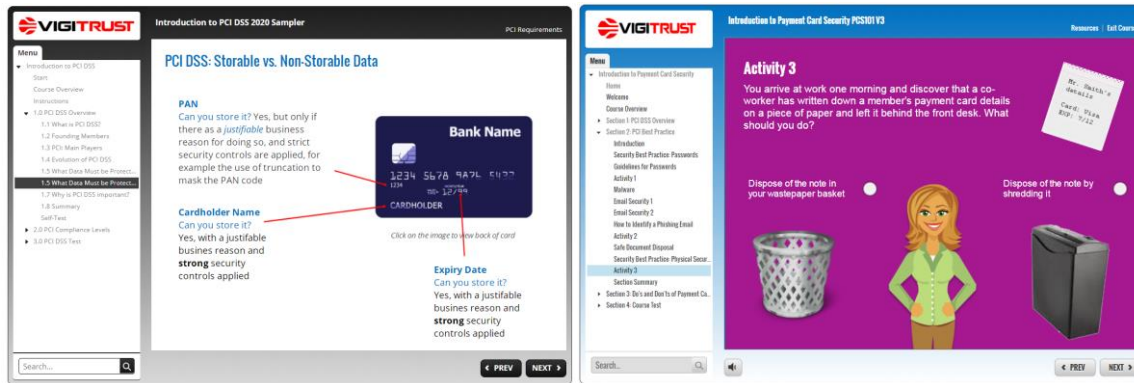
- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-MT
- SAQ D
- SAQ D-IP
- SAQ P2PE
- RESET SAQ LIST

VigiOne as Merchant Compliance Platform for PCI DSS is a web-based platform created to allow merchants to quickly and simply validate compliance with PCI DSS (Payment Card Industry Data Security Standards) which they are required to do by their acquiring bank and the card service providers' regulations. It has been created by VigiTrust and partners security and compliance experts. The MCP includes a suite of features that simplifies and centralizes the compliance process for any merchant, group of merchants or organization wishing to demonstrate compliance to PCI DSS.

VigiOne is modular and configurable. VigiOne is designed to enable organisations to manage compliance to multiple data standards and information security regulations with one single program and platform. This often means that such organisations start using VigiOne to manage to one single security standard and then evolve to add others as appropriate. One common and very successful concept has been to use VigiOne to manage compliance to PCI DSS. In such a case, the features of VigiOne are very specific to PCI DSS.

Using the MCP, the merchant will provide access to a number of key features required to validate compliance:

eLearning: educate staff as to what PCI DSS is and how to protect card holder data and confidential information by providing a course for a number of appropriate staff.



Policy and procedure management tool: This tool allows for the tracking of alignment and standardization of policy and procedures where possible, with local, regional and functional variation where required. The system comes preloaded with some standard PCI DSS policy templates that are relatively easy for merchants to customize for the own use. The MCP enables merchants to download and assign a status to generic security polices (i.e. in place/not in place). All documents are based on VigiTrust templates. Merchants or organizations can upload their own versions of these policies or other relevant policies as required. (This module can be customized for non-standard set-ups, contact VigiTrust for more information).

SAQ Completion functionality: The HCP has in-built versions of all SAQs and guides merchants to the SAQ they need to complete by asking them key questions about how they take credit card payments. Merchants can complete the SAQs online and download print out and/or mail the completed documents.

MCP allows the generation and completion of all of the PCI DSS SAQ Types for merchants and Service Providers;

SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C-VT, SAQ, SAQ P2PE, SAQ D for Merchants & SAQ D for Service Providers.

Where required merchants can upload a current in force PCI DSS SAQ or AOC from alternative source.

Document/Evidence Library: MCP includes a Secure Evidence Library, where files containing documentation, reports, images, statistics, vulnerability scans etc. can be stored as evidence and dynamically linked to requirements, controls and tasks. This includes the capability to set up, store and track Compensating Controls as dictated by the regulations.

Evidence Library

Documentation / Documents / Evidence Library

Export as CSV View Evidence Library Role

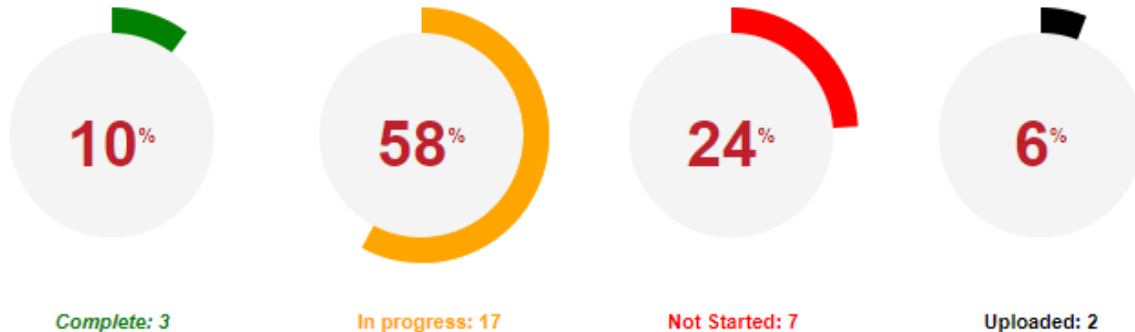
Show 10 entries Search:

Document Name	File extension	Used as Evidence	Date uploaded	Client	Download
Review Document Data Risk Migration & Mitigation Plan	pdf	5	2019-02-08 11:53:52		Download
Review Document Formal Risk Mitigation and Migration Plan	docx	8	2018-12-05 13:09:37		Download
Review Document POS Inspector Approval	docx	15	2018-12-05 10:09:09		Download

Assessment Review & Tracking Feature: The MCP allows internal and external assessors to review self assessments (SAQ) and provide advisory and validation services where required. The system maintains a complete audit trail of all review comments and conclusions.

Workflow Tool: The system includes a task assignment and management tool with calendar, allowing users to set up one-off and recurring tasks that can be assigned to individual users and business units with priorities and deadlines. These can be used to manage and track compliance and remediation activity, but also to ensure, that re-occurring tasks such as training, testing, vulnerability scanning and SAQ completion are scheduled and managed.

Dashboard and reports: Full reporting, configured by user type, and with dynamic features for customization and drill down. Full data export functionality for more detailed analysis. The reporting feature can be customized at the request of the client, tracking compliance across thousands of merchants often in diverse industries or spread across many countries, currencies, languages etc. Multi-level dashboards with statistics, trends and charts again with drill down and export functionality.



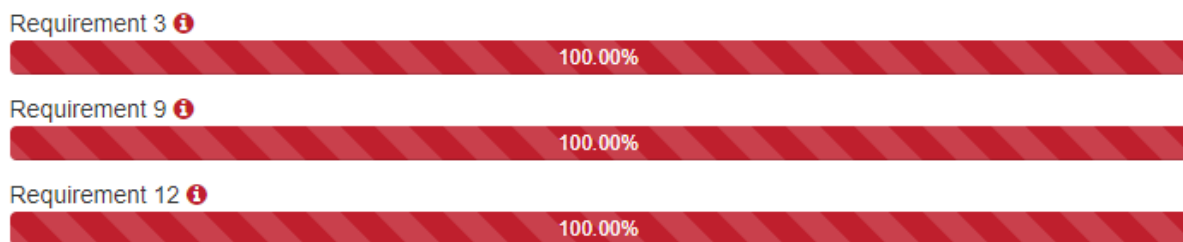
Organization & User Management: Multilevel organisational and user management with features such as self-service user management, authentication and single sign-on where required.

VigiOne for SAQ Generation & Management Features:

SAQ P2PE - 2019 [redacted] Ticket Sales and Donations [redacted] m0052 ×

General information: *Inplace: 30 | Not in place: 0 | Not Applicable: 3 | Compensating: 0 | Not tested: 0*

Executive summary: **Set as Complete**



AOC: **Set as Complete**

SAQ Comment (last comment from R.Hegarty)

Applies to MIDs: 1503 [redacted] 99 ([redacted] Ticket) and 150 [redacted] 97 ([redacted] Ticket)

[Access SAQ](#) [Close](#)

SAQ Management Tool

- Allows the merchant to create a suitable PCI DSS SAQ assessments as required. Also includes access to VigiTrust's PCI DSS eLearning Modules and access to the VigiOne Policy and Procedures Management Module.
- Provide the functionality for project managers to input planned remediation date for requirements that are not in place in response to SAQ questions

Evidence Library

On completion of SAQ questions users can upload files based on the responses to the questions, these include;

- Evidence of testing and compliance (test results, reports, policies, checklists etc.)
- Explanations for non-tested and not applicable responses
- Compensating Control Worksheets where required
- Photos, Screen Pics, data files etc.

Tasks and deadlines

The user can assign tasks to the business units or as part of creating a remediation plan

Access to eLearning and Awareness

- PCI DSS Introduction and/or Credit Card Security (potentially course could be appropriately customized for merchants based on the payment systems and services that they are using)

Access to Assessments

- Access to the default SAQ wizard to select the SAQ Type (again this could be customized for a PSP directing merchant to appropriate SAQ for payment service in use.
- Access to the SAQ in English (Executive summary, Requirements, AOC), can be customized for other languages, based on support from the PCI Council.
- Upload of multiple proof of evidence per requirement
- Link uploaded document(s) to multiple requirements and SAQs
- Generation of SAQ in PDF
- Generation of AOC in PDF

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ C (Section 2), dated (2020-10-28).

Based on the results noted in the SAQ C dated (2020-10-28), 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 (2020-10-28): **(check one)**

Compliant: All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall **COMPLIANT** rating, thereby (Town of Apex) 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 (Town of Apex) 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 exceptions: 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
<input type="button" value="Add Entry"/>	

Part 3a. Acknowledgement of Status

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

PCI DSS Self-Assessment Questionnaire C, Version (3.2.1), 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.

No evidence of full track data¹, CAV2, CVV2, CID, or CVV2 data², or PIN data³ 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)

Note:

¹ 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.

² 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.

³ Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.

Part 3b. Merchant Attestation

Access to dashboard

- User management system (add, edit users)
- eLearning and awareness quick report
- Assessment quick report
- SAQ review and action plan default features
- Document evidence uploaded report per SAQ
- Policies and Procedures quick report
- Overall Status Report
- Default Charts
- Default Export customized report as PDF

Access to Calendar / task / remediation plan

- Assign a task to a specific entity

- Category, frequency and task template

Access to standard Assistance

- Request assistance module
- User Guide

Standard Vigione Reports

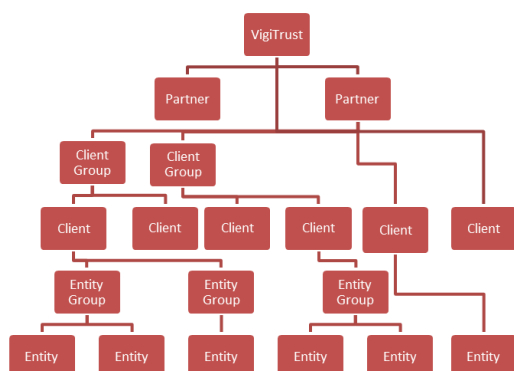
Reports include PCI DSS Documents and Overview of PCI Assessments

Vigione Roles and Organisation Structure

Additional Technical Information:

- Vigione MCP application annual subscriptions are licensed based on the number of SAQs, entities and users in the system, as further described in the Vigione Terms of Use and the related Vigione Order Form.
- Vigione supports the following web browsers: Internet Explorer 11.43 for Windows, Safari for Apple systems, Android and IOS (including iPad all tablets, desktops, mobile) and Google Chrome. Generally speaking Vigione supports browser versions that remain supported by their producers.
- Vigione Software UI is based in English, but has been delivered in other languages on request.
- User accounts within the application are defined by roles. Roles with appropriate security access are created at the group level.

- Data is stored in a multi-tenant instance of



Vigione Software.

- Permission based user access based on role controls what documents a user may access.

General:

- User guides will be made available in accordance with the current versions as they become available. User guides will be made available upon setup of the platform.

The above information, as provided by Vigione, is a summarized version and is intended to highlight the controls, policies, processes and procedures that are applicable to the particular SaaS service, its functionality and how it is architected. Such information, as current as of this point-in-time, may be updated periodically.

Institution	Roles	Modules
Vigitrust	Administrator	eLearning Course
Partner	Program Manager	Assessments
Client Group	Assessor	Documentation
Client	Project Manager	Polices and Procedures
Entity Group	Entity Manager	Surveys
Entity	Assistant	Dashboards
	Alternate Contact	Organization Management
	Staff	Calendar / Tasks