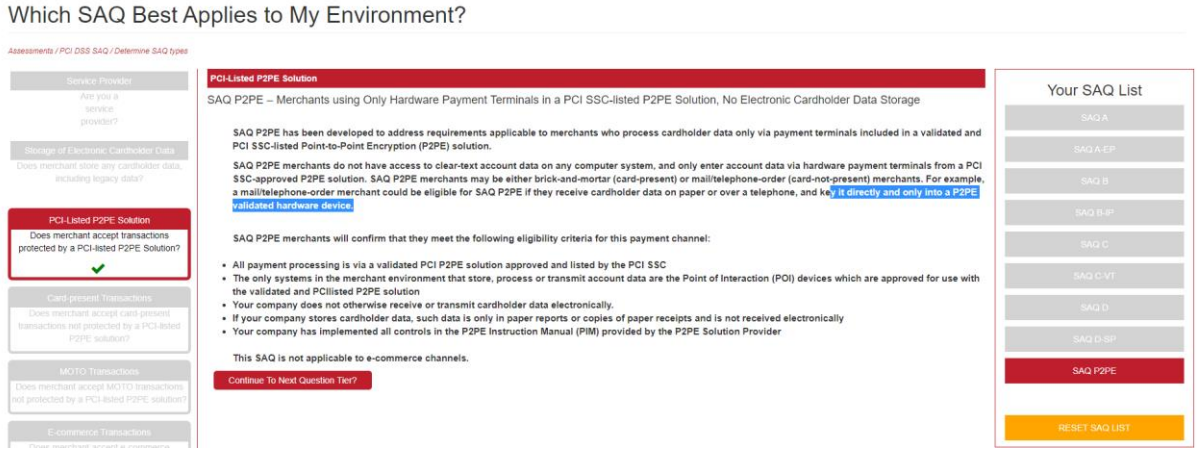
Overview

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

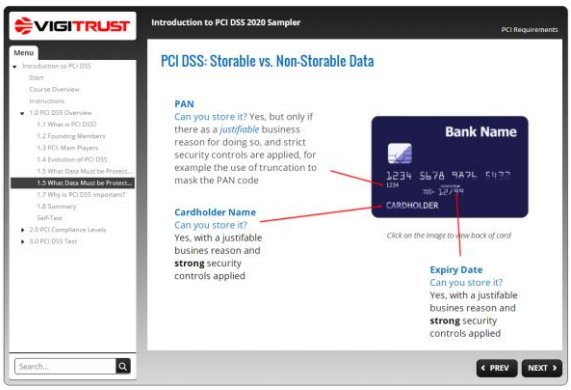


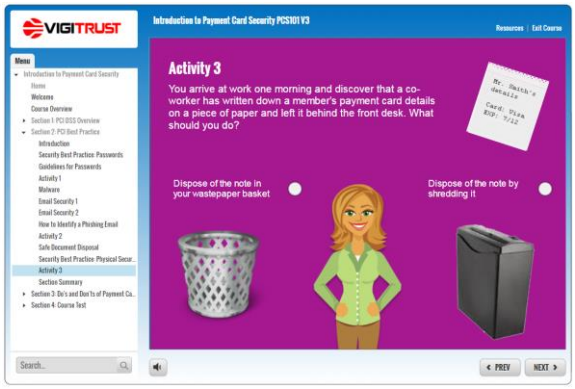
VigiOne as Merchant Compliance Platform for PCI DSS is a web-based platform created to allow merchants to quickly and simply validate compliance with PCI DSS (Payment Card Industry Data Security Standards) which they are required to do by their acquiring bank and the card service providers' regulations. 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 alll 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.

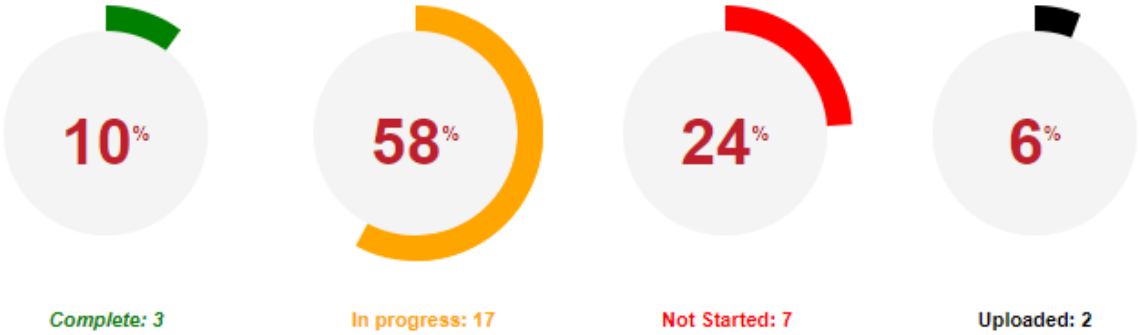
Where required merchants can upload a current in force PCI DSS SAQ or AOC from alternative source.

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.

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.

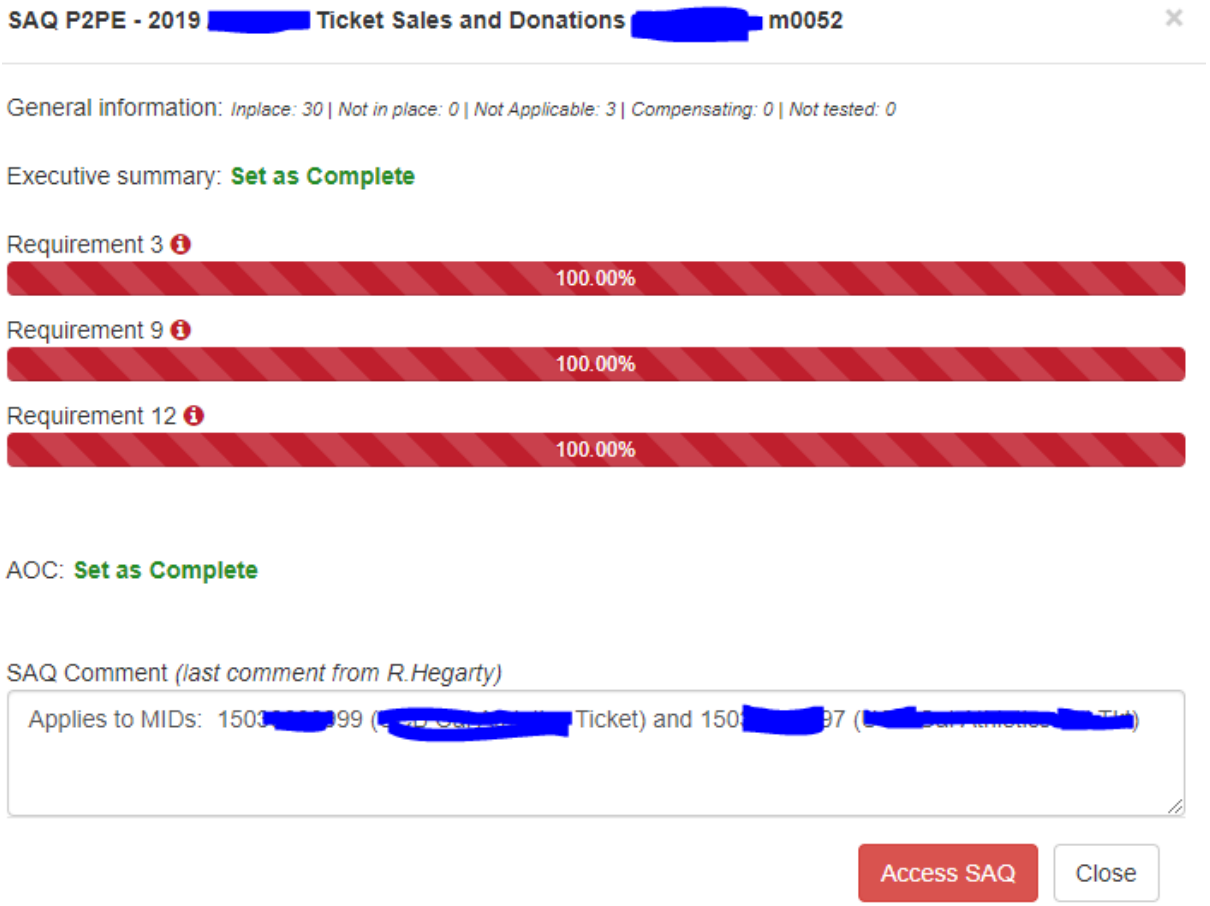
Workflow Tool: The system includes a task assignment and management tool with calendar, allowing users to set up one-off and recurring tasks that can be assigned to individual users and business units with priorities and deadlines. These can be used to manage and track compliance and remediation activity, 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 customixed 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 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

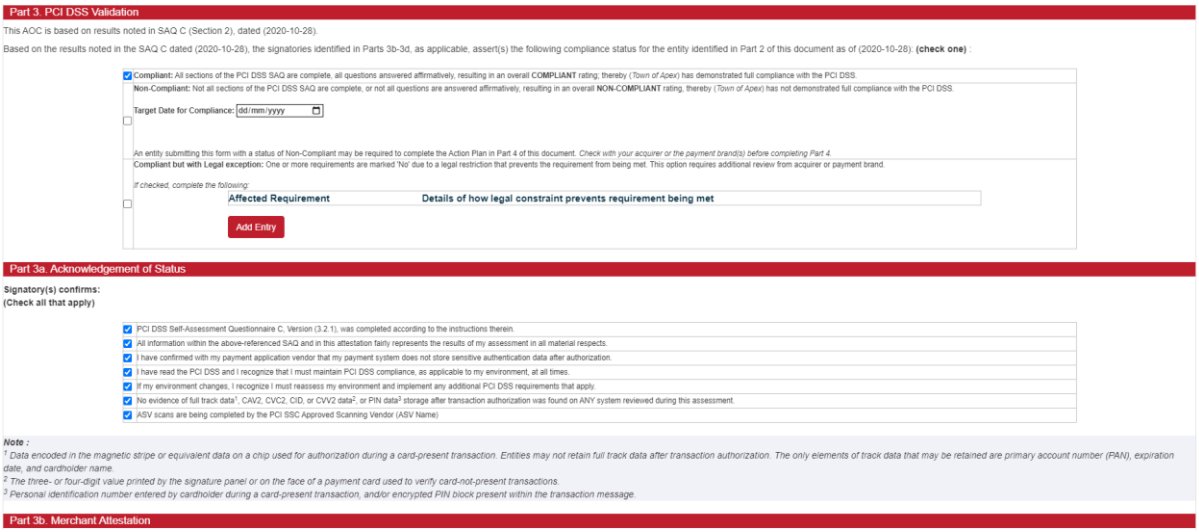
The user can assign tasks to the business units or as part of creating a remediation plan

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



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

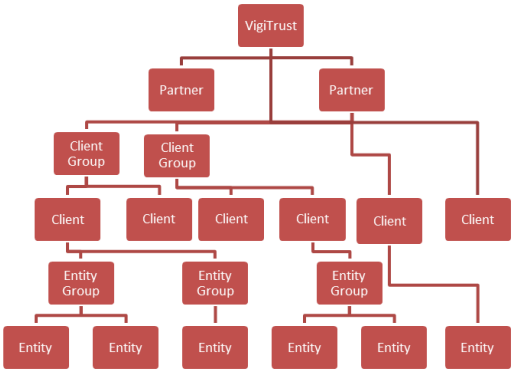
Standard VigiOne Reports

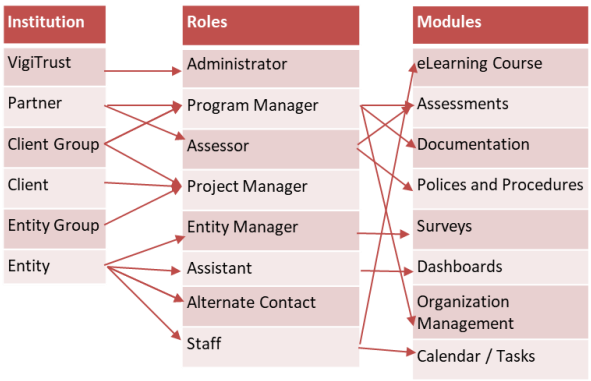
Reports include PCI DSS Documents and Overview of PCI Assessments

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.