

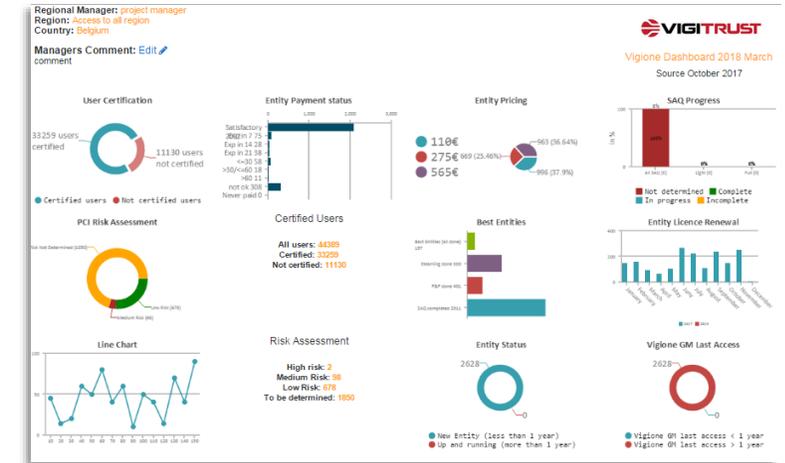
VigiOne Overview PCI SAQ Tool



VigiOne is Available to Coalfire Clients

Tools and resources:

- VigiOne for PCI
 - SAQ Tool
 - eLearning
 - Policies & Procedures Repository
 - Dashboard
 - Reporting
- Full eLearning Portfolio



Which SAQ Best Applies to My Environment?

PCI-Listed P2PE Solution

P2PE Merchants

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

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.

Continue to Next Question Test?

Your SAQ List

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-EP
- SAQ C
- SAQ C-EP
- SAQ D
- SAQ P2PE

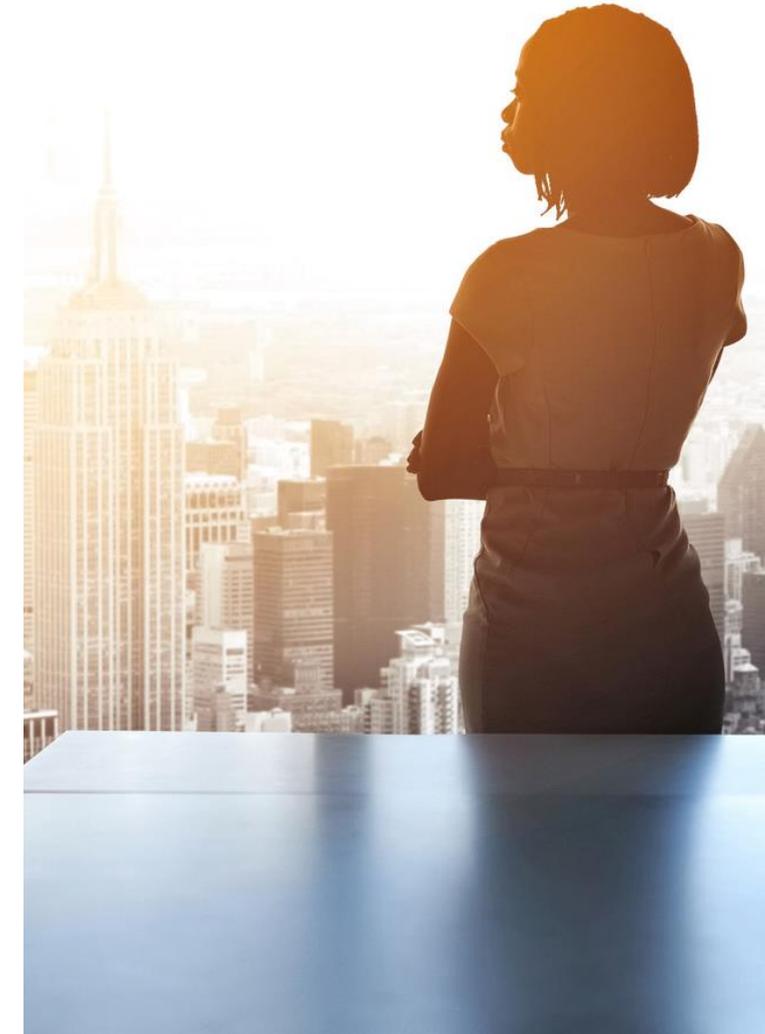
Benefits of VigiOne for PCI Compliance

- Presents a single unified view of PCI DSS compliance across the organization for clients
 - whether you're a small merchant or a complex multi-level organization
- Manages and tracks workflows and progress through task scheduling and smart dashboards
- Allows you to clearly identify and specify areas and actions for improvement in compliance
- Creates a central repository of all data and information management requirements, controls, measures and documentary evidence for provision to QSAs, consultants, acquiring banks, card issuers, or representatives of any regulator



VigiOne Overview

1. SAQ Completion and Management
2. Secure Evidence Library
3. User Management Features
4. Reporting and Dashboards
5. Policy and procedure management tool
6. Integrated learning management system (LMS)
7. Task assignment and management tool
8. Role driven access rights and features
9. Multi-level help desk system
10. Access to additional features
 - online purchasing opportunity



VigiOne Home

VIGITRUST project manager | Project Manager | pjm0001 | US

Welcome to VigiOne

- New Comments: 0** [View Details](#)
- New Tasks: 0** [View Details](#)
- New Orders: 0** [View Details](#)
- Support Tickets: 0** [View Details](#)

VigiOne Overview Report - 2018-03-27

Number of users total: 778
Number of countries: 1
Number of entities: 58
New created users: 0
New created entities: 0
Logged in Vigione: 4

SAQ Management

- Access all 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
- Use clever wizards to determine which SAQs are appropriate for in-scope Organizations



SAQ Management

Click on a questionnaire to modify questions

- ◊ SAQ A (22 questions) - Delete
- ◊ SAQ A-EP (192 questions) - Delete
- ◊ SAQ B (38 questions) - Delete
- ◊ SAQ B-IP (83 questions) - Delete
- ◊ SAQ C-VT (83 questions) - Delete
- ◊ SAQ C (160 questions) - Delete
- ◊ SAQ P2PE (33 questions) - Delete
- ◊ SAQ D (330 questions) - Delete

Total : 8 questionnaires

Create a new SAQ

Create a new SAQ based on a template



SAQ Wizard – Determine Which SAQ

The screenshot shows the VIGITRUST SAQ Wizard interface. The top navigation bar includes the VIGITRUST logo, a user profile for 'Toto McToto | Project Manager | PM001 | US', and notification icons. The left sidebar contains a menu with items: eLearning & Awareness, Assessments, Policies & Procedures, Vulnerability Scan, Surveys, Asset Management, Dashboard, Calendar / Tasks, and Assistance. The main content area is titled 'Which SAQ Best Applies to My Environment?' and features a series of questions in a vertical column on the left. The first question, 'PCI-Listed P2PE Solution', is highlighted with a red border and a green checkmark, indicating it is the selected path. Below this question is a red button labeled 'Continue To Next Question Tier?'. The main content area is titled 'PCI-Listed P2PE Solution' and contains the following text: 'P2PE Merchants' and 'SAQ P2PE merchants will confirm that they meet the following eligibility criteria for this payment channel:'. A list of criteria follows: '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', and 'Your company has implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider'. Below the list, a paragraph explains that 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. The right sidebar, titled 'Your SAQ List', contains a vertical list of SAQ options: SAQ A, SAQ A-EP, SAQ B, SAQ B-IP, SAQ C, SAQ C-VT, SAQ D, and SAQ P2PE. The SAQ P2PE option is highlighted with a red background.

VIGITRUST Toto McToto | Project Manager | PM001 | US

Which SAQ Best Applies to My Environment?

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-presents 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?

PCI-Listed P2PE Solution

P2PE Merchants

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

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.

[Continue To Next Question Tier?](#)

Your SAQ List

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D
- SAQ P2PE**

Access the SAQ Wizard by selecting the Assessments drop down box, select PCI DSS SAQ and Determine SAQ types to begin.

- eLearning & Awareness <
- Assessments >
- PCI DSS SAQ >**
 - Determine SAQ types
 - Manage SAQ Templates
 - Manage Consolidated SAQ
 - Assessment Management
- Documentation <
- Policies & Procedures <
- Organization Management <
- Calendar / Tasks <
- Assistance <

WHICH SAQs Best Apply to My Environment?

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

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

-
-
-
-
-
-
-
-
-

SAQ Management

The screenshot shows the VIGITRUST SAQ Management interface. The top navigation bar includes the VIGITRUST logo, a notification icon, a user icon, and the text "project manager | Project Manager | pjm0001 | US". The left sidebar contains a menu with items: eLearning & Awareness, Assessments, Policies & Procedures, Vulnerability Scan, Surveys, Dashboard (with a "Filter active" indicator), Calendar / Tasks, and Assistance. The main content area is titled "Add a new SAQ to My Environment?". It features a "Service Provider" section with a red header and a white box containing the question "Are you a service provider?" with a green checkmark below it. Below this are two grey boxes: "Storage of Electronic Cardholder Data" with the question "Does merchant store any cardholder data, including legacy data?" and "PCI-Listed P2PE Solution" with the question "Does merchant accept transactions protected by a PCI-listed P2PE Solution?". A red button labeled "Click here to start the SAQ D" is positioned below the second grey box. To the right, under the "Service Provider" header, is the "Service Providers" section. It includes the text "Examples of merchant environments that would use SAQ D may include but are not limited to:" followed by a bulleted list: "E-commerce merchants who accept cardholder data on their website", "Merchants with electronic storage of cardholder data", "Merchants that don't store cardholder data electronically but that do not meet the criteria of another SAQ type", and "Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment." Below the list is a paragraph: "While many organizations completing SAQ D will need to validate compliance with every PCI DSS requirement, some organizations with very specific business models may find that some requirements do not apply. For example, a company that does not use wireless technology in any capacity would not be expected to validate compliance with the sections of the PCI DSS that are specific to managing wireless technology."

Manage your PCI DSS SAQ

If SAQ Type is already known, go to Manage SAQ Templates and select the Add a new template tab. In the drop down box select the template and give it a name and select Create.

- eLearning & Awareness <
- Assessments >
- PCI DSS SAQ >
 - Determine SAQ types
 - Manage SAQ Templates
 - Manage Consolidated SAQ
 - Assessment Management
- Documentation <
- Policies & Procedures <
- Organization Management <
- Calendar / Tasks <
- Assistance <

Edit your current templates

Add a new template to your current selection

Edit Template name

Assign template to Entity

Duplica

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

Create the selected SAQ template



Access any existing SAQs by selecting Manage SAQ Templates and the tab for Edit your current templates



Manage your PCI DSS SAQ templates

- eLearning & Awareness <
- Assessments >
- PCI DSS SAQ >**
 - Determine SAQ types
 - Manage SAQ Templates
 - Manage Consolidated SAQ
 - Assessment Management
- Documentation <
- Policies & Procedures <
- Organization Management <
- Calendar / Tasks <
- Assistance <

- Edit your current templates**
- Add a new template to your current selection
- Edit Template name
- Assign template to Entity
- Duplicate e>

Manage your current SAQ templates

➔ Access template SAQ A (2019)

OR

Manage previously Assigned SAQs



SAQ Pre-population & Customization



welcome, project manager

[Go back to VigiOne](#)

Questions selection for : SAQ D

1 - Requirement 1

- 1.1.1** ✓ Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations
- 1.1.2.a** ✓ Is there a current network diagram that documents all connections between the cardholder data environment and other networks, including any wireless networks?
- 1.1.2.b** ✓ Is there a process to ensure the diagram is kept current?
- 1.1.3.a** ✓ Is there a current diagram that shows all cardholder data flows across systems and networks?
- 1.1.3.b** ✓ Is there a process to ensure the diagram is kept current?
- 1.1.4.a** ✓ Is a firewall required and implemented at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone?

330 / 348 selected

SAVE

[Back to SAQ management](#)

- 1.1.1 x 1.1.2.a x 1.1.2.b x 1.1.3.a x 1.1.3.b x 1.1.4.a x
- 1.1.4.b x 1.1.5 x 1.1.6.a x 1.1.6.b x 1.1.7.a x 1.1.7.b x
- 1.2.1.a x 1.2.1.b x 1.2.2 x 1.2.3 x 1.3.1 x 1.3.2 x
- 1.3.3 x 1.3.4 x 1.3.5 x 1.3.6 x 1.3.7.a x 1.3.7.b x
- 1.4.a x 1.4.b x 1.5 x 2.1.1.a x 2.1.1.b x 2.1.1.c x
- 2.1.1.d x 2.1.1.e x 2.1.a x 2.1.b x 2.2.1.a x 2.2.1.b x
- 2.2.2.a x 2.2.2.b x 2.2.3 x 2.2.4.a x 2.2.4.b x 2.2.4.c x
- 2.2.5.a x 2.2.5.b x 2.2.5.c x 2.2.a x 2.2.b x 2.2.c x
- 2.2.d x 2.3.a x 2.3.b x 2.3.c x 2.3.d x 2.4.a x
- 2.4.b x 2.5 x 3.1.a x 3.1.b x 3.1.c x 3.1.d x
- 3.1.e x 3.2.1 x 3.2.2 x 3.2.3 x 3.2.c x 3.3 x 3.4 x
- 3.4.1.a x 3.4.1.b x 3.4.1.c x 3.5.2 x 3.5.3 x 3.5.4 x
- 3.6.1 x 3.6.2 x 3.6.3 x 3.6.4 x 3.6.5.a x 3.6.5.b x
- 3.6.5.c x 3.6.6 x 3.6.7 x 3.6.8 x 3.6.a x 3.7 x



SAQ Requirements

3.1.a Is data storage amount a

Please select an answer

Please select an answer ▼

Please select an answer

Not Tested

In Place

Not in Place

Not Applicable

Compensating

In Place ▼

3.1.b Are there defined processes in place

Not Tested ▼

PCI Manager comment

Requirement Approved:

Project Manager Comment:

Remediation date:

Additional information

Testing Procedures

Review policies and procedures

Interview personnel

Examine deletion mechanism

SAQ Requirements – Not Applicable

3.1.e Does all stored cardholder data meet the requirements defined in the data-retention policy?

Not Applicable ▼

If you choose Not Applicable (NA), please state the reason(s) why this requirement does not apply to your Merchant.

submit

If you choose Not Applicable, you can upload proofs of evidence :

Upload a document

SAQ Requirements Assessment

SAQ B Assessment Questionnaire

Executive summary AOC Requirement 3 Requirement 4 Requirement 7 (2 / 2) Requirement 9 Requirement 12

Requirement 7 - Number of responses : 2 / 2

Filters : All No answer (0) Not tested (0) In place (1) Not in place (1) Not applicable (0) Compensating (0)

7.1.2 Is access to privileged user IDs restricted as follows:
To least privileges necessary to perform job responsibilities?
Assigned only to roles that specifically require that privileged access?

Not in Place

If you choose Not in place (NO), please state the reason(s) why this requirement is not in place.

If you choose Not in place, you can insert a remediation date :
Planned remediation date :

submit

Progress Requirement 7 (SAQ B)
100.0%

Questions
Questions completed by entity

Question Status Legend
 Not Tested
 In Place
 Not in Place
 Not Applicable
 Compensating

Download SAQ
[SAQ B 3.2](#)

SAQ Requirements Compensating Controls

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.	

Close

- 📖 eLearning & Awareness <
- 📄 Assessments <
- 📋 Policies & Procedures <
- 🔍 Vulnerability Scan <
- 📊 Surveys <
- 🏠 Dashboard 📌 Filter active <
- 📅 Calendar / Tasks <
- 📄 Assistance <

SAQ Attestation of Compliance

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

This appendix is not used for merchant assessments.

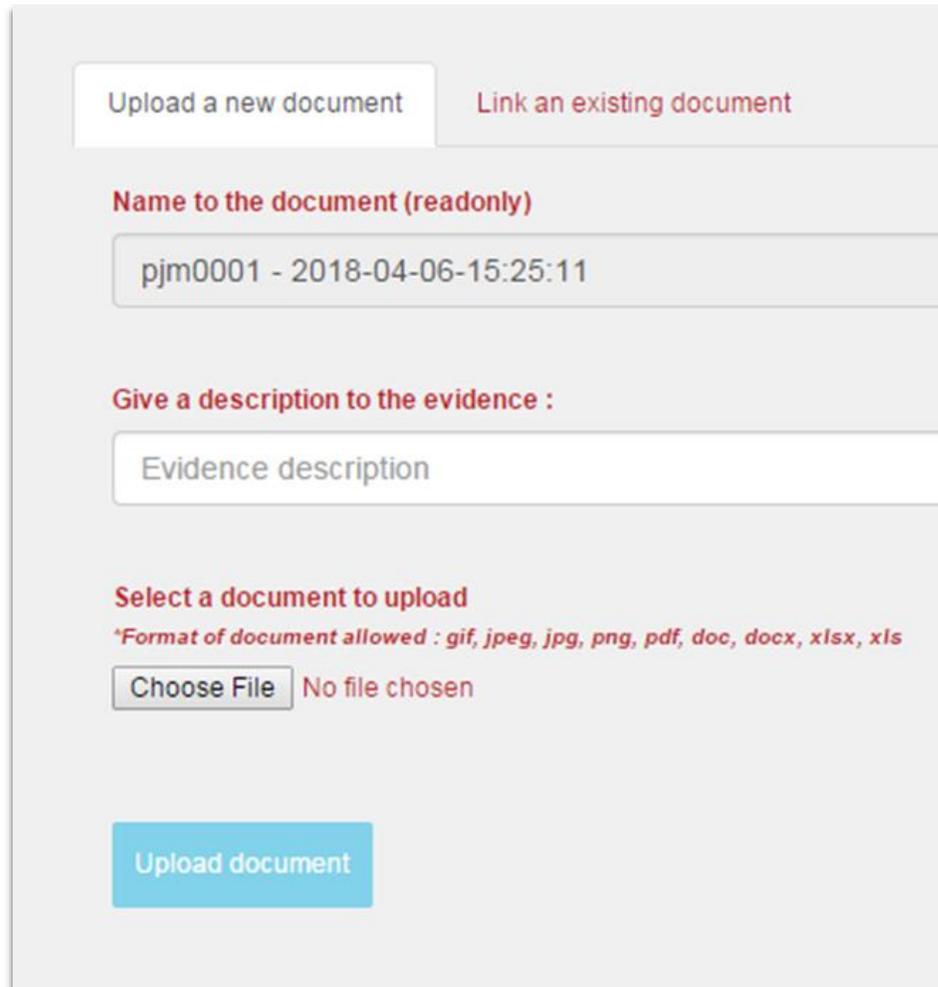
Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

Submit the Attestation of Compliance

	PCI DSS Question	Expected Testing	Response(Check one response for each question)				
A2.1	<p>For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:</p> <ul style="list-style-type: none"> Are the devices confirmed to not be susceptible to any known exploits for SSL/early TLS <p>Or:</p> <ul style="list-style-type: none"> Is there a formal Risk Mitigation a 	Review documentation (for example, vendor documentation system/network configuration details, etc.) that verifies POS POI devices are not susceptible to any known exploits for SSL/early TLS	yes: <input type="radio"/>	yes with CCW: <input type="radio"/>	no: <input type="radio"/>	n/a: <input type="radio"/>	not tested: <input type="radio"/>
A2.2	<p>Is there a formal Risk Mitigation and Migration Plan in place for all implementations that use SSL and/or early TLS (other than as allowed in A2.1), that includes:</p> <ul style="list-style-type: none"> Description of usage, including: what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; Risk assessment results and risk reduction controls in place; Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; Overview of migration project plan including target migration completion date no later than 30th June 2018? 	Review the documented Risk Mitigation and Migration Plan	yes: <input type="radio"/>	yes with CCW: <input type="radio"/>	no: <input type="radio"/>	n/a: <input type="radio"/>	not tested: <input type="radio"/>

Appendix B: Compensating Controls Worksheet

Secure Evidence Library



The screenshot shows a web form for uploading a document. At the top, there are two buttons: "Upload a new document" (highlighted in white) and "Link an existing document" (in red). Below these is a section for document details. The first field is "Name to the document (readonly)" with a text input containing "pjm0001 - 2018-04-06-15:25:11". The second field is "Give a description to the evidence :" with a text input containing "Evidence description". Below this is a section for file selection. It says "Select a document to upload" and lists allowed formats: "gif, jpeg, jpg, png, pdf, doc, docx, xlsx, xls". There is a "Choose File" button and the text "No file chosen". At the bottom of the form is a large blue "Upload document" button.

- Store files containing documentation, reports, images, statistics, vulnerability scans etc. can be as evidence
- Documents dynamically linked to requirements, controls and tasks.
- Includes the capability to set up, store and track Compensating Controls as dictated by the regulations

User Management

Add a new user

Username	Firstname	Lastname	Email	Country	Finalgrade	Training Status	Certification date	User registration	User last access	Edit User	Assign Task
m9999entity	entity	fest	vigitrust@vigitrust.com	US	0	Incomplete		23/03/2018	26/04/2018		
a	toto	tata	vigitrust@vigitrust.com	US	0	Incomplete		10/04/2018			

Assign a Task to entity demo

Category:

Frequency:

Reload tasks:

Task Title:

All day

Starts:

Ends:

Description:

M0000 Manage entity demo Settings

Edit

Edit Details

Username (in lowercase,Maximum 30 characters) :	<input type="text" value="m0000entity"/>
Firstname:	<input type="text" value="entity"/>
Lastname:	<input type="text" value="demo"/>
Email:	<input type="text" value="vigitrust@vigitrust.com"/>

Multilevel organizational and user management with features such as self-service user management, authentication and single sign-on where required

Reporting and Dashboards



- Full reporting, configured by user type and with dynamic features for customization and drill down
- Full data export functionality for more detailed analysis
- Customized for organizations tracking compliance across thousands of merchants often in diverse industries or spread across many countries, currencies, and languages
- Multi-level dashboards with statistics, trends, and charts again with drill down and export functionality

SAQ Complete Report

SAQ complete:

Show entries

Search:

Entity Code	Entity Name	Country	mtype	Entity Type	Region	SAQ status	SAQ type	SAQ:number of question answered
M0467	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M0840	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M0864	vigione	Franchised	vigone	Belgium	BENELUX	Complete	A	105
M0958	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M0961	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M1030	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M1033	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M1046	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M1047	vigione	Subsidiary	vigone	Belgium	BENELUX	Complete	A	105
M1071	vigione	Managed	vigone	Belgium	BENELUX	Complete	A	105

Showing 1 to 10 of 49 entries

Previous **1** 2 3 4 5 Next

Global Overview Report

Global Overview Report

Last update of data : 2017/09/12 08:30:00am GMT (Update every 12 hours)

Show 10 entries

Search:

Entity Code ^{↑↓}	Users registered ^{↑↓}	Users certified ^{↑↓}	P&P in place ^{↑↓}	P&P not in place ^{↑↓}	P&P not applicable ^{↑↓}	SAQ status ^{↑↓}	SAQ type ^{↑↓}	SAQ: number of question answered ^{↑↓}
M0467	30	25	23	1	1	Complete	A	105
M0840	23	23	23	1	1	Complete	A	105
M0864	8	8	17	0	1	Complete	A	105
M0958	13	13	23	1	1	Complete	A	105
M0961	16	12	20	3	2	Complete	A	105
M1030	24	24	24	0	1	Complete	A	105
M1033	26	26	23	0	1	Complete	A	105
M1046	17	12	23	1	2	Complete	A	105
M1047	14	14	24	0	2	Complete	A	105
M1071	35	32	14	1	0	Complete	A	105
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Showing 1 to 10 of 58 entries

Previous **1** 2 3 4 5 6 Next

Other Key Features of VigiOne

- **Integrated learning management system (LMS)**
 - Links awareness and understanding with policy implementation
 - Interactive, multilingual eLearning courses with testing and certification
 - PCI DSS eLearning tailored for multiple user types, payment staff, program managers, technical staff, senior executives, merchants, and franchisees
- **Policy and procedure management tool**
 - Tracks alignment and standardization of policies and procedures with local, regional, and functional variations where required
 - PCI DSS policy templates that are easy to customize for your own use can be pre-loaded

Other Key Features of VigiOne

- **Task assignment and management tool**
 - Calendar allows users to set up one-off and recurring tasks, assignable to individual users and business units with priorities and deadlines.
 - Tasks can be used to manage and track compliance and remediation activity
 - Ensure that recurring tasks such as training, testing, and SAQ completion are scheduled and managed
- **Role driven access rights and features**
 - Users only see and have access to the functionality that they need based on their role and responsibility
 - Higher level users can drill down as needed

Other Key Features of VigiOne

- **Multi-level help desk system**

- Users can raise issues within VigiOne, and management can track response and resolution
- User guides, instructional videos, and FAQs are also available

- **Access to additional features – online purchasing opportunity**

- Online purchasing function that allows users set up and pay for annual subscriptions where required
- Additional modules can be purchased within VigiOne as and when needed
- Automated notification and tracking of subscription renewals, reminders, rebates, discounts, and payments

Steps for a Smooth Transition

1. Contact Coalfire or VigiTrust to migrate to VigiOne.
2. Set up a user account and subscription with VigiTrust.
3. Your SAQ data will be imported into your new system automatically.
4. Review your data to confirm that it migrated correctly and edit as needed.*

For immediate queries please contact: VigiOne@vigitrust.com

~~SAQSupport@coalfire.com~~ ~~SAQSupport@vigitrust.com~~



** Note: Older SAQ reports may need to be downloaded by you for recordkeeping purposes.*

