



# Payment Card Industry Data Security Standard

---

## **Attestation of Compliance for Self-Assessment Questionnaire D for Service Providers**

**For use with PCI DSS Version 4.0**

Revision 2

Publication Date: August 2023



## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the entity's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures*. Complete all sections: The entity is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Self-Assessment Questionnaire (SAQ).

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Self-Assessment Questionnaire.

### Part 1. Contact Information

#### Part 1a. Assessed Entity

Company name:	Vaultera ehf.
DBA (doing business as):	Vaultera, Channex PCI
Company mailing address:	Iceland, 220, Hafnarfjörður, Miðvangi 159
Company main website:	<a href="https://vaultera.co">https://vaultera.co</a>
Company contact name:	Sigurjón Ernir Kárasón
Company contact title:	CEO
Contact phone number:	+3548203525
Contact e-mail address:	Sigurjon@vaultera.co

#### Part 1b. Assessor

Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.

##### PCI SSC Internal Security Assessor(s)

ISA name(s):	
Qualified Security Assessor	
Company name:	Compliance Control ltd
Company mailing address:	Estonia, 13619, Harju, Tallinn, Punane tn. 16/1-409
Company website:	<a href="https://compliance-control.eu">https://compliance-control.eu</a>
Lead Assessor Name:	Evgeny Maslakov
Assessor phone number:	+372 600 44 64
Assessor e-mail address:	e.maslakov@compliance-control.eu
Assessor certificate number:	205-606



## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment (select all that apply):**

Name of service(s) assessed:		Technology solution provider	
Type of service(s) assessed:			
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):		<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	
<input type="checkbox"/> Account Management <input type="checkbox"/> Back-Office Services <input type="checkbox"/> Billing Management <input type="checkbox"/> Clearing and Settlement <input type="checkbox"/> Network Provider <input type="checkbox"/> Others (specify):		<input type="checkbox"/> Fraud and Chargeback <input type="checkbox"/> Issuer Processing <input type="checkbox"/> Loyalty Programs <input checked="" type="checkbox"/> Merchant Services	
		<input type="checkbox"/> POI / card present <input checked="" type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):	
		<input checked="" type="checkbox"/> Payment Gateway/Switch <input type="checkbox"/> Prepaid Services <input type="checkbox"/> Records Management <input type="checkbox"/> Tax/Government Payments	

**Note:** These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.



## Part 2. Executive Summary *(continued)*

### Part 2a. Scope Verification *(continued)*

**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment** (select all that apply):

Name of service(s) not assessed:

-

Type of service(s) not assessed:

Hosting Provider:	Managed Services:	Payment Processing:
<input type="checkbox"/> Applications / software	<input type="checkbox"/> Systems security services	<input type="checkbox"/> POI / card present
<input type="checkbox"/> Hardware	<input type="checkbox"/> IT support	<input type="checkbox"/> Internet / e-commerce
<input type="checkbox"/> Infrastructure / Network	<input type="checkbox"/> Physical security	<input type="checkbox"/> MOTO / Call Center
<input type="checkbox"/> Physical space (co-location)	<input type="checkbox"/> Terminal Management System	<input type="checkbox"/> ATM
<input type="checkbox"/> Storage	<input type="checkbox"/> Other services (specify):	<input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Web-hosting services		
<input type="checkbox"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Multi-Tenant Service Provider		
<input type="checkbox"/> Other Hosting (specify):		
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:	-	

### Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Vaultera is a connectivity platform for hotels, Channel Managers, PMS and other hotel tech vendors. The entity is a technology solution provider for tokenized e-commerce transactions. The entity uses AWS services to store, process and transmits account data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Entity doesn't involve in any additional process impacting security of cardholder data.
Describe system components that could impact the security of account data.	No any other system components that has the ability to impact the security of cardholder data were indicated.



**Part 2. Executive Summary** *(continued)*

**Part 2c. Description of Payment Card Environment**

Provide a **high-level** description of the environment covered by this assessment.

*For example:*

- *Connections into and out of the cardholder data environment (CDE).*
- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

CDE consist of dedicated CDE segments inside AWS. All the segmentation is done with the firewalls. Only several employees can connect to the servers in the AWS via remote access. All users are connected to the CDE with remote access 2FA. All connections from partners uses strong cryptography.

Indicate whether the environment includes segmentation to reduce the scope of the assessment.

*(Refer to “Segmentation” section of PCI DSS for guidance on segmentation.)*

Yes  No

**Part 2d. In-Scope Locations/Facilities**

List all types of physical locations/facilities—for example, corporate offices, data centers, call centers, and mail rooms—in scope for the PCI DSS assessment.

Facility Type	Total number of locations (How many locations of this type are in scope)	Location(s) of facility (city, country)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Head Office	1	Hafnarfjörður, Iceland
IaaS, PaaS cloud service-provider	1	Amazon Web Services (AWS)



## Part 2. Executive Summary *(continued)*



**Part 2e. PCI SSC Validated Products and Solutions**

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions\*?

Yes  No

Provide the following information regarding each item the entity uses from PCI SSC’s Lists of Validated Products and Solutions.

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)

\* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org))—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.



## Part 2. Executive Summary *(continued)*





## Part 2f. Third-Party Service Providers

For the services being validated, does the entity have relationships with one or more third-party service providers that:

<ul style="list-style-type: none"> <li>Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>Manage system components included in the scope of the entity's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>Could impact the security of the entity's CDE—for example, vendors providing support via remote access, and/or bespoke software developers.</li> </ul>	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

### If Yes:

Name of service provider:	Description of service(s) provided:
Amazon Web Services (AWS)	IaaS, PaaS cloud service-provider
Booking.com B.V	Online Travel Agent
Agoda	Online Travel Agent
Hostelworld	Online Travel Agent
Expedia	Online Travel Agent
Hotelier 101	Property Management System
Ermes Hotels	Property Management System
Turkey Protel	Property Management System
Paycomet	Property Management System
Revenatium	Property Management System

**Note:** Requirement 12.8 applies to all entities in this list.



## Part 2. Executive Summary *(continued)*

### Part 2g. Summary of Assessment

*(SAQ Section 2 and related appendices)*

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either “Not Applicable” or “Not Tested,” complete the “Justification for Approach” table below.

**Note:** One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: Technology solution provider

PCI DSS Requirement	Requirement Responses				
	<i>More than one response may be selected for a given requirement. Indicate all responses that apply.</i>				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Justification for Approach



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.3.3 No wireless networks are used.</p> <p>2.2.5 No insecure services, protocols and daemons are used.</p> <p>2.3 There are no wireless environments connected to cardholder data environment or transmitting cardholder data.</p> <p>3.3.3 The entity do not participate in issuing services in any role.</p> <p>3.5.1.2 There are no full-disk encryption are used.</p> <p>3.7.6 Manual cleartext cryptographic key-management operations are not performed by entity's personnel.</p> <p>4.2.1.2 There are no wireless environments connected to cardholder data environment or transmitting cardholder data.</p> <p>4.2.2 The entity does not use end-user messaging technologies to send cardholder data.</p> <p>8.2.3 No remote access to customers premises is used.</p> <p>8.2.7 Remote access to entity's environment is not available for vendors.</p> <p>9.4.3-9.4.4 No media with CHD are sent outside the facility.</p> <p>9.5 The entity doesn't use devices that capture payment card data via direct physical interaction.</p> <p>Appendix A1 - The entity is not a multi-tenant service provider.</p> <p>Appendix A2 - The entity doesn't use SSL/early TLS. Requirements and/or individual bullets which are considered best practice until 31.03.2024 and 31.03.2025 are marked as Not Applicable.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>-</p>



## Section 2: Self-Assessment Questionnaire D for Service Providers

---

Self-assessment completion date:	2024-03-28
Were any requirements in the SAQ unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date 2024-03-28).

Indicate below whether a full or partial PCI DSS assessment was completed:

- Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.
- Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document.

Select one:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Vaultera ehf.</i> has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted <i>before completing Part 4.</i></p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby (<i>Service Provider Company Name</i>) has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.</p> <p>This option requires additional review from the entity to which this AOC will be submitted. <i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



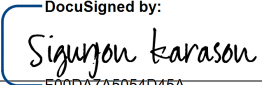
### Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

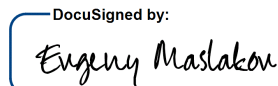

(Select all that apply)

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version 4.0 was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced SAQ and in this attestation fairly represents the results of the entity's assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

### Part 3b. Service Provider Attestation

DocuSigned by:  F00DA7A5054D45A...	
Signature of Service Provider Executive Officer ↑	Date: 2024-03-28
Service Provider Executive Officer Name: <b>Sigurjón Ernir Kárason</b>	Title: <b>CEO</b>

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	<input checked="" type="checkbox"/> QSA performed testing procedures.
	<input type="checkbox"/> QSA provided other assistance. If selected, describe all role(s) performed:
DocuSigned by:  7E1831545D5E4E0...	
Signature of Lead QSA ↑	Date: 2024-03-28
Lead QSA Name: <b>Evgeny Maslakov</b>	
DocuSigned by:  BFF44B14139C478...	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2024-03-28
Duly Authorized Officer Name: <b>Evgeny Babitskiy</b>	QSA Company: <b>Compliance Control Ltd.</b>

### Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	<input type="checkbox"/> ISA(s) performed testing procedures.
	<input type="checkbox"/> ISA(s) provided other assistance. If selected, describe all role(s) performed:



## Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the entity expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If “NO” selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	N/A
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	N/A

