



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024



PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: OneTrust, LLC

Date of Report as noted in the Report on Compliance: November 30, 2025

Date Assessment Ended: October 6, 2025



Section 1: Assessment Information

Instructions for Submission

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

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

Part 1a. Assessed Entity (ROC Section 1.1)

Company name:	OneTrust, LLC
DBA (doing business as):	Not applicable.
Company mailing address:	505 North Angier Avenue NE, Suite 9000, Atlanta, GA 30308
Company main website:	www.onetrust.com
Company contact name:	Adrienne Canter
Company contact title:	Sr. Director GRC & Data Protection
Contact phone number:	470-607-3631
Contact e-mail address:	adrienne.canter@onetrust.com

Part 1b. Assessor (ROC Section 1.1)

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):	Not applicable
Qualified Security Assessor	
Company name:	Schellman Compliance, LLC
Company mailing address:	4010 W Boy Scout Boulevard, Suite 600, Tampa, FL 33607
Company website:	https://www.schellman.com/services/pci-compliance
Lead Assessor name:	Phil Dorczuk
Assessor phone number:	866.254.0000 ext. 161
Assessor e-mail address:	pciocs@schellman.com
Assessor certificate number:	QSA (202-889)



Part 2. Executive Summary

Part 2a. Scope Verification

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

Name of service(s) assessed: OneTrust Platform

Type of service(s) assessed:

<p>Hosting Provider:</p> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input checked="" 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): Not applicable.	<p>Managed Services:</p> <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): Not applicable.	<p>Payment Processing:</p> <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): Not applicable.
<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): Not applicable.		

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 Assessment (select all that apply):

Name of service(s) not assessed:	Not applicable.	
Type of service(s) not assessed:		
Hosting Provider: <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): Not applicable.	Managed Services: <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): Not applicable.	Payment Processing: <input type="checkbox"/> POI / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify): Not applicable.
<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): Not applicable.		
Provide a brief explanation why any checked services were not included in the Assessment:	Not applicable.	

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	OneTrust is a Software as a Service (SaaS) provider. The OneTrust Platform provides customers a central portal to collect, organize, and share their governance, risk management, and compliance data. As part of this service offering, OneTrust's customers may upload data that contains cardholder data. OneTrust does not process any credit cards in the scope of this assessment. Any transmission of cardholder data is incidental to the functioning of the platform and OneTrust has no visibility into the data provided by customers. Customers utilizing the
---	---



	<p>platform to store cardholder data are fully responsible for redacting, encrypting/decrypting, and retention of that data.</p>
<p>Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.</p>	<p>Not applicable. OneTrust is responsible for the architecture underlying its SaaS offering that runs in Microsoft Azure but customers are responsible for the data that they provide to the portal.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>The following critical system components within the CDE were assessed:</p> <ul style="list-style-type: none"> - Azure management console - Linux operating systems Support Systems - Multi-factor authentication - Change Management - File Integrity Monitoring - Intrusion Detection Systems - Logging and Alerting - Configuration Management



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.*

The OneTrust platform may be used by customers to send or receive data containing cardholder data. Customer data provided to the platform is sent over an encrypted TLS v1.2 tunnel with strong cryptography. Customers utilizing the platform to store cardholder data are fully responsible for redacting, encrypting/decrypting, and retention of that data. OneTrust does not process any credit cards in the scope of this assessment.

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

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

Yes No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Azure Regions	28	Australia East, Australia Southeast, Brazil South, Canada Central, Canada East, Central India, Central US, East Asia, East US, East US 2, France Central, France South, Germany North, Germany West, Germany West Central, Japan West, Japan West, North Europe, Southeast Asia, South India, Switzerland North, Switzerland West, UAE Central, UAE North, UK South, UK West, West Europe, West US



Part 2. Executive Summary (continued)

Part 2e. PCI SSC Validated Products and Solutions (ROC Section 3.3)

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
Not applicable.	Not applicable.	Not applicable.	Not applicable.	Not applicable.

* 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) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

♦ 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)—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
(ROC Section 4.4)

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"> • 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)) 	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
<ul style="list-style-type: none"> • Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers) 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

If Yes:

Name of Service Provider:	Description of Services Provided:
Microsoft Azure	Cloud service provider
Splunk	Cloud logging solution for the CDE

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



Part 2. Executive Summary (continued)

Part 2g. Summary of Assessment (ROC Section 1.8.1)

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: OneTrust Platform

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

1.2.6: OneTrust did not maintain any insecure services, protocols, or ports.
 1.3.3, 2.3.1, 2.3.2, 11.2.2: OneTrust had no wireless networks connected to the in-scope environment.
 1.4.4, 3.1.1-3.7.9, 4.2.1, 4.2.1.1, 4.2.1.2, 4.2.2, 7.2.6, 9.4.1-9.4.7, 10.2.1.1: OneTrust did not store, process, or access cardholder data.



Part 2. Executive Summary (continued)

	<p>5.2.3, 5.2.3.1: Antivirus software was implemented for system components capable of installing such software.</p> <p>5.3.2.1: OneTrust did not rely on periodic malware scans to meet requirement 5.3.2. Real-time, heuristic-based detection was performed.</p> <p>6.4.3, 11.6.1: OneTrust did not have any payment pages in the scope of this assessment.</p> <p>6.5.5: OneTrust did not develop any applications that store, transmit, or process cardholder data. No card data was used when developing the application.</p> <p>8.2.3: No remote access to customer premises was available to users.</p> <p>8.3.9: OneTrust deployed multi-factor authentication on all in-scope systems.</p> <p>8.3.10, 8.3.10.1: OneTrust did not provide customer access to cardholder data.</p> <p>9.5.1-9.5.1.3, A2.1.1-A2.1.3: OneTrust did not maintain any card interaction devices.</p> <p>10.4.2: All system components within the OneTrust in-scope environment were logged to Splunk Cloud.</p> <p>11.3.1.3-11.3.2.1: No significant changes occurred to the in-scope environment during the previous 12 months.</p> <p>11.4.4: No exploitable risks were identified in the initial penetration testing results.</p> <p>11.4.7, A1.1.1-A1.2.3: OneTrust was not a multi-tenant service provider.</p> <p>12.3.2: The customized approach was not utilized to fulfill any requirements in this assessment.</p> <p>12.5.3: No significant changes to OneTrust's organization structure occurred during the previous 12 months.</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>Not applicable.</p>



Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>	September 6, 2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	October 6, 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *November 30, 2025*.

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

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

Based on the results documented in the ROC 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*):

- Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *OneTrust, LLC* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
- Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *OneTrust, LLC* has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance: Not applicable

 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 before completing Part 4.
- Compliant but with Legal exception:** One or more assessed requirements in the ROC 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 In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *OneTrust, LLC* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction.

 This option requires additional review from the entity to which this AOC will be submitted.

If selected, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement from being met



Part 3. PCI DSS Validation (continued)

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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

Signed by:

Adrienne Canter

8F819A100F6447D...

Signature of Service Provider Executive Officer ↑

Date: 12/1/2025

Service Provider Executive Officer Name: Adrienne Canter

Title: Sr. Director GRC & Data Protection

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:

QSA performed testing procedures.

QSA provided other assistance.

If selected, describe all role(s) performed: Not applicable.

DocuSigned by:

Phil Dorczuk

A4B3D04D20164FC...

Signature of Lead QSA ↑

Date: 12/1/2025

Lead QSA Name: Phil Dorczuk

DocuSigned by:

Adam Bush

4C64E1964742453...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 12/1/2025

Duly Authorized Officer Name: Adam Bush

QSA Company: Schellman Compliance, LLC

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

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:

ISA(s) performed testing procedures.

ISA(s) provided other assistance.

If selected, describe all role(s) performed: Not applicable.



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 Non-Compliant results 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 provide 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"/>	Refer to part 2g for requirement applicability.
2	Apply secure configurations to all system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
3	Protect stored account data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
5	Protect all systems and networks from malicious software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
6	Develop and maintain secure systems and software	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
7	Restrict access to system components and cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
8	Identify users and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
10	Log and monitor all access to system components and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
11	Test security systems and networks regularly	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
12	Support information security with organizational policies and programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Refer to part 2g for requirement applicability.

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/