



Payment Card Industry Data Security Standard

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

For use with PCI DSS Version 4.0.1

Revision 1

Publication Date: December 2024

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:	Wingify Software Pvt. Ltd.
DBA (doing business as):	VWO
Company mailing address:	703, 7th floor, KLJ North Tower, Netaji Subhash Place, Pitampura, Delhi-110034, India
Company main website:	www.vwo.com
Company contact name:	Keshav Kumar
Company contact title:	Data Protection Officer
Contact phone number:	9034272875
Contact e-mail address:	privacy@vwo.com

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):	NA
--------------	----

Qualified Security Assessor

Company name:	Cybersigma Consulting Services LLP
Company mailing address:	4th Floor, Majestic Signia, 405, Plot No. A-27, Block A, Industrial Area, Sector 62, Noida, Uttar Pradesh 201309
Company website:	https://cybersigmacs.com
Lead Assessor Name:	Abhay Singh
Assessor phone number:	+91 9717016127
Assessor e-mail address:	abhay@cybersigmacs.com
Assessor certificate number:	206-681

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: VVO Experience Optimization Platform and its related infra		
Type of service(s) assessed:		
Hosting Provider: <input checked="" 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 checked="" type="checkbox"/> Other Hosting (specify): Software as a Services (SaaS) based delivery of JS Smartcode and SDKs for the VVO Experience Optimization Platform.	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):	Payment Processing: <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 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):		

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:	Services those are mentioned in above section are excluded in this section
----------------------------------	--

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):	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):	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):
<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:		NA

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.

Wingify Software Pvt. Ltd., founded in 2010 and based out of New Delhi, India is a forward thinking software company known for its innovative SaaS product, "VWO Experience Optimization Platform", which enables businesses to optimize their websites through A/B testing and other data-driven tools. Wingify is a global SaaS company building experience optimization tools for businesses with online visitors, trusted by brands across 90 countries. Wingify's mission is to Empower its customers with cutting-edge conversion optimization technology, fostering closer connections with their audience. Wingify is committed to enhancing key performance metrics, ensuring wins at every touchpoint, and building a sustainable future together. Wingify places a strong emphasis on information security,

	<p>privacy, and compliance, having earned several key certifications, including ISO 27001:2022 ISMS, ISO 27701:2019 PIMS, ISO 27017 Cloud Security, and ISO 27018 Cloud Privacy. With a dedicated Corporate Security and Compliance team and a robust data protection framework led by a Data Protection Officer, Wingify continuously ensures that its products and operations meet global standards for security and privacy.</p> <p>The PCI DSS established at Wingify Software Pvt Ltd applies the integration code i.e JS Smartcode and SDKs required for 'VWO Experience Optimization Platform'.</p> <p>i. As a service provider, Wingify requires its customers to add a JS Smartcode & SDK on their websites for using its SaaS product 'VWO Experience optimization platform'. While Wingify does not store, process and/or transit this data, it still has the ability to impact the security of such cardholder data.</p> <p>ii. As a service provider to its customers, wingify collects payments through its merchant (Verifone (dba 2checkout)) for the purchased subscription. Even though Wingify does not have the ability to directly impact cardholder data, Wingify's merchant (Verifone (dba 2checkout)) as the third-party service provider of such transactions has the ability to impact the security of cardholder data.</p> <p>The company doesn't store process or transmit CHD.</p>
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	No CHD is stored, processed or transmitted
Describe system components that could impact the security of account data.	Same as above

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

<p>Provide a high-level description of the environment covered by this assessment.</p> <p><i>For example:</i></p> <ul style="list-style-type: none"> • <i>Connections into and out of the cardholder data environment (CDE).</i> • <i>Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.</i> • <i>System components that could impact the security of account data.</i> 	<ol style="list-style-type: none"> 1. GCP infrastructure. 2. Entity Application
Indicate whether the environment includes segmentation to reduce the scope of the assessment.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

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

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>
Corporate Office	1	Wingify Software Pvt. Ltd., 703, 7th floor, KLJ North Tower, Netaji Subhash Place, Pitampura, Delhi-110034, India

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)—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.

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"> 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 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. 	<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 service(s) provided:
GCP	Cloud Service Provider

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: VWO Experience Optimization Platform and its related infra

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 type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input 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 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>1.2.8 - The requirement is not applicable because the entity has deployed their servers over the GCP and GCP cloud is PCI DSS Certified.</p> <p>1.3.3 - This requirement is not applicable as there is no wireless network in the environment as they have their network over the GCP Cloud</p> <p>2.2.5 - This requirement is not applicable because there are no insecure services, protocols, or daemons are present.</p> <p>2.3 - The accessor has verified that the client is having their servers over the AWS Cloud and there is no wireless technology in use.</p> <p>Requirement 3 - Not applicable because entity doesn't store PAN and SAD data.</p> <p>Requirement 4 - Not Applicable as entity doesn't transmit any CHD.</p> <p>5.2.3 - Entity has deployed anti malware solution on all of its inscope servers</p> <p>6.3.2, 6.4.2, 6.4.3 - No Payment page is managed by entity</p> <p>7.2.6 - No CHD stored, processed or transmitted</p> <p>8.3.10 - No CHD stored, processed or transmitted</p> <p>Requirement 9 - Not Applicable because data hosted on GCP.</p> <p>10.2.1.1 - NO CHD stored, processed or transmitted</p> <p>11.2.2 - No Wireless device in the network</p> <p>11.2 - No wireless technology in use</p> <p>11.4.5 - Segmentation is not used</p> <p>11.4.6 - Segmentation is not used</p> <p>11.4.7 - Entity is not a multi tenant service provider</p> <p>11.6 - No payment page provided by the entity</p> <p>12.3.2 - No customized approach used for targeted risk analysis</p> <p>12.10.7 - No CHD stored, processed or transmitted</p>
<p>For any Not Tested responses, identify which sub-requirements were not tested and the reason.</p>	<p>NA</p>

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2025-05-07
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 2025-05-07).

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>Compliant: 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 COMPLIANT rating; thereby <i>Wingify Software Pvt. Ltd.</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>Non-Compliant: 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 NON-COMPLIANT rating, thereby (<i>Service Provider Company Name</i>) has not demonstrated compliance with the PCI DSS requirements included in this SAQ.</p> <p>Target Date 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>Compliant but with Legal exception: 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 COMPLIANT BUT WITH LEGAL EXCEPTION 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"> <thead> <tr> <th>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 4.0.1, 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



Signature of Service Provider Executive Officer ↑	Date: 2025-05-12
Service Provider Executive Officer Name: Sparsh Gupta	Title: CEO

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:



Signature of Lead QSA ↑	Date: 2025-05-12
Lead QSA Name: Abhay Singh	



Signature of Duly Authorized Officer of QSA Company ↑	Date: 2025-05-12
Duly Authorized Officer Name: Sharwan Jha	QSA Company: Cybersigma Consulting Services

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:

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 checked="" type="checkbox"/>	<input type="checkbox"/>	
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"/>	

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 its program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/.