Security Standards Council®

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:	Instructure, Inc.
DBA (doing business as):	Not Applicable
Company mailing address:	6330 S 3000 E #700, Cottonwood Heights, UT 84121
Company main website:	https://www.instructure.com
Company contact name:	Deepa Talreja
Company contact title:	Director, Security Compliance
Contact phone number:	800.203.6755
Contact e-mail address:	security@instructure.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):	Not Applicable
Qualified Security Assessor	
Company name:	Moss Adams
Company mailing address:	999 Third Ave. #2800, Seattle, WA 98104
Company website:	https://mossadams.com
Lead Assessor Name:	Trevor Lapointe
Assessor phone number:	214.242.7420
Assessor e-mail address:	trevor.lapointe@mossadams.com
Assessor certificate number:	QSA, 206-680

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:	Instructure Canvas Catalog Payment Redirector/iFrame
Type of service(s) assessed:	

Hosting Provider:	**Managed Services:**	**Payment Processing:**
□ Applications / software □ Hardware □ Infrastructure / Network □ Physical space (co-location) □ Storage □ Web-hosting services □ Security services □ 3-D Secure Hosting Provider □ Multi-Tenant Service Provider □ Other Hosting (specify):	□ Systems security services □ IT support □ Physical security □ Terminal Management System □ Other services (specify):	□ POI / card present ☒ Internet / e-commerce □ MOTO / Call Center □ ATM □ Other processing (specify):
□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
□ 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:	Other components of Canvas Catalog
Type of service(s) not assessed:	

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	□ Systems security services	□ POI / card present
□ Hardware	□ IT support	□ Internet / e-commerce
□ Infrastructure / Network	□ Physical security	□ MOTO / Call Center
□ Physical space (co-location)	□ Terminal Management System	□ ATM
□ Storage	□ Other services (specify):	□ Other processing (specify):
□ Web-hosting services		
□ Security services		
□ 3-D Secure Hosting Provider		
□ Multi-Tenant Service Provider		
□ Other Hosting (specify):		
□ Account Management	□ Fraud and Chargeback	□ Payment Gateway/Switch
□ Back-Office Services	□ Issuer Processing	□ Prepaid Services
□ Billing Management	□ Loyalty Programs	□ Records Management
□ Clearing and Settlement	□ Merchant Services	□ Tax/Government Payments
□ Network Provider		
□ Others (specify):		

Provide a brief explanation why any checked services were not included in the assessment:	The Instructure Canvas Catalog Payment Redirector/iFrame Service was a separate service from the rest of the Canvas Catalog SaaS product, including the code base and the hosting environment. Changes to the rest of the Canvas Catalog SaaS product did not affect the security of the Payment Redirector Service.

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	Instructure does not store, process, or transmit cardholder data.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Instructure's Canvas Catalog product allows users to select courses that require a fee in order to take the course. When the user has completed their selection of courses to purchase, the user is redirected to a payment provider (or, in one case, is redirected to an iFrame) where the user inputs their payment information to complete the purchase. The software service that handles this redirection is called Canvas Catalog Payment Redirector. When the payment is successful,

	the Payment Redirector receives confirmation from the payment provider that the payment was successful. Canvas Catalog allows the student to proceed with the purchased content. Therefore, cardholder data originates at a user's browser and is transmitted directly to a third-party payment processor along with payment details, bypassing Instructure's systems. Since Instructure serves the HTML where the third-party iFrame is included or which includes the link to the third-party payment processor's site, certain PCI Requirements apply to its environment.
Describe system components that could impact the security of account data.	Instructure's web environment which serves the HTML that serves up the third-party iFrame, as well as all authentication mechanisms and maintenance processes to support the environment.

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.*	In-scope processes include the collection of payments that were accepted via third-party payment processors via an iFrame or URL Redirects. Payment card data flowed directly from the user's browser to payment processor servers. The iFrame/URL Redirect references were hosted on servers within AWS. The iFrame/URL Redirect processes above helped make sure that no cardholder data was stored, processed, or transmitted by design by Instructure. Technologies in use include the following: - Ecommerce website and iFrame/URL Redirect - Linux web servers serving web code
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)
Example: Data centers	*3*	*Boston, MA, USA*
Data centers	4	AWS US East AWS AP Southeast AWS CA Central AWS EU Central

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)
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, 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:

• 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)	□ Yes ☒ No
• 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.	☒ Yes □ No
• Could impact the security of the entity's CDE—for example, vendors providing support via remote access, and/or bespoke software developers.	☒ Yes □ No

If Yes:

Name of service provider:	**Description of service(s) provided:**
Amazon Web Services	Infrastructure-as-a-Service (IaaS)
(Payment Processors)	(Payment processors were not included as "Instructure service providers" since Instructure integrated with payment processors upon request of Instructure clients. Instructure clients managed the relationship with the payment processors.)

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: Instructure Canvas Catalog Payment Redirector/iFrame

PCI DSS Requirement	**Requirement Responses** *More than one response may be selected for a given requirement.* *Indicate all responses that apply.*				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☐	☐	☒	☐	☐
Requirement 2:	☒	☐	☒	☐	☐
Requirement 3:	☐	☐	☒	☐	☐
Requirement 4:	☐	☐	☒	☐	☐
Requirement 5:	☐	☐	☒	☐	☐
Requirement 6:	☒	☐	☒	☐	☐
Requirement 7:	☐	☐	☒	☐	☐
Requirement 8:	☒	☐	☒	☐	☐
Requirement 9:	☐	☐	☒	☐	☐
Requirement 10:	☒	☐	☒	☐	☐
Requirement 11:	☒	☐	☒	☐	☐
Requirement 12:	☒	☐	☒	☐	☐
Appendix A1:	☐	☐	☒	☐	☐
Appendix A2:	☐	☐	☒	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.1.1 - 1.5.1, 2.1.1 - 2.2.1, 2.2.3 - 2.3.2, 5.1.1 - 5.4.1, 6.1.1 - 6.2.4, 6.3.2, 6.4.1, 6.4.2, 6.5.1 - 6.5.6, 7.1.1 - 7.3.3, 8.1.1, 8.1.2, 8.2.4, 8.2.6 - 8.2.8, 8.3.2, 8.3.8, 8.3.11 - 8.6.3, 10.1.1 - 10.6.3, 11.1.1 - 11.3.1.3, 11.4.1 - 11.4.5, 11.5.1 - 11.5.2, 12.1.1 - 12.3.4, 12.5.1, 12.5.3 - 12.7.1, 12.10.2 - 12.10.7 : Instructure's scope of services is not applicable to these requirements. 3.1.1 - 3.7.9, 9.4.1, 9.4.1.1, 9.4.2 - 9.4.4, 9.4.5.1, 9.4.6 : Instructure does not store account data. 4.1.1 - 4.2.2 : Instructure does not transmit account data. 6.4.3, 11.6.1, 12.5.2.1 : Instructure opted not to test best practice requirements this year. 6.5.2, 11.3.2.1 : Instructure had no significant changes this year. 8.2.3 : Instructure did not have access to customer premises. 8.3.9 : MFA is required for all access to the environment. 8.3.10, 8.3.10.1 : Instructure's customers did not have remote access to the environment. 9.1.1 - 9.4.7: Instructure did not have physical access to cardholder data. 9.5.1 - 9.5.1.3, Appendix A2 : Instructure's scope of services did not utilize POI devices. 10.7.2, 10.7.3 : Instructure did not experience any security control failures. 11.4.6 : Segmentation is not used. 11.4.7, Appendix A1 : Instructure is not a multi-tenant service provider.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2024-06-10
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ 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 *2024-06-10***).**

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:

☒ **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 *Instructure, Inc.* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.

☐ **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 *(Service Provider Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ.

Target Date for Compliance: *YYYY-MM-DD*

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 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 *(Service Provider Company Name)* 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.

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 3a. Service Provider Acknowledgement

Signatory(s) confirms:
(Select all that apply)

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

Part 3b. Service Provider Attestation

DocuSigned by:
Deepa Talreja
67B7BA1FAA76428...

Signature of Service Provider Executive Officer ↑	*Date:* 6/12/2024
Service Provider Executive Officer Name: **Deepa Talreja**	*Title:* **Director, Security Compliance**

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:

DocuSigned by:
Trevor Lapointe
412276C6B1E944B...

Signature of Lead QSA ↑	*Date:* 6/12/2024

Lead QSA Name: **Trevor Lapointe**

DocuSigned by:
Jonathan Smith
2D38ED022A9D4EB...

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* 6/12/2024
Duly Authorized Officer Name: **Jonathan Smith**	*QSA Company:* **Moss Adams LLP**

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