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: Arbor Education Partners Limited

Date of Report as noted in the Report on Compliance: 17 August 2026

Date Assessment Ended: 31 July 2026

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:	Arbor Education Partners Limited
DBA (doing business as):	Arbor Education
Company mailing address:	Floor 4, FORA, 21-33 Great Eastern Street,, London, EC2A 3EJ
Company main website:	www.arbor-education.com
Company contact name:	Damian Brooks
Company contact title:	CTO
Contact phone number:	+44(0) 7754 746 408
Contact e-mail address:	damian.brooks@abor-education.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:	Cyber Security Associates Limited
Company mailing address:	Unit 11, Wheatstone Court, Waterwells Business Park, Gloucester, Gloucestershire, GL2 2AQ, UK
Company website:	https://csacyber.com
Lead Assessor name:	James Cullen
Assessor phone number:	+44 (0) 7591 338 506
Assessor e-mail address:	james.cullen@csacyber.com
Assessor certificate number:	206-561

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:	Arbor Education Management Infomration System (MIS)	
Type of service(s) assessed:		
Hosting Provider: ☐ 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):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ 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 Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable	
Type of service(s) not assessed:		
Hosting Provider: ☐ 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):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ 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):		
Provide a brief explanation why any checked services were not included in the Assessment:		

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.	Arbor Education provides a payment capability within its SaaS platform that enables its customers (schools and educational institutions) to accept payments from parents, guardians, and other payers. When a payer chooses to make a payment through the Arbor application, they are directed to a Stripe-hosted Checkout page where payment card details are entered and processed directly by Stripe.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	All payment transactions are outsourced to Stripe and utilise the same Stripe-hosted Checkout mechanism as when Arbor is acting as a merchant. Cardholder data is entered directly into Stripe's payment environment and

	does not pass through, nor is it stored within, Arbor's systems. Consequently, Arbor's payment model is based on a fully outsourced payment architecture whereby all payment card processing activities are performed by Stripe
Describe system components that could impact the security of account data.	Although the payment processing is provided by Stripe the redirection method to Stripe is controlled and maintained by Arbor Education. These redirection servers are hosted within AWS but access and authentication, vulnerability and patch management, change control is all within Arbor Educations control which may affect the security of Account Data

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.*	Arbor Education operates both as a merchant and as a third-party service provider within the payment ecosystem. As a service provider, Arbor provides payment functionality within its SaaS platform, enabling its customers, including schools and educational institutions, to accept payments from parents, guardians, and other payers. The payment channel utilises Stripe Checkout, a PCI DSS-compliant hosted payment solution. For both Arbor's own payments and payments accepted on behalf of its customers, users are redirected to Stripe hosted payment pages where payment card data is entered and processed directly by Stripe. Arbor does not store, process, or transmit payment card data within its own environment. Following successful transaction processing, limited transaction details are returned to the Arbor platform to support payment reconciliation, reporting, and account management functions. Arbor is responsible for the security of the e commerce application, supporting infrastructure, and integration with Stripe, while Stripe is responsible for the secure collection, transmission, processing, and storage of payment card data in accordance with the documented shared responsibility model.
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)
Example: Data centers	*3*	*Boston, MA, USA*
N/A	N/A	N/A

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.

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:

• 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 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)	☒ 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 Services Provided:
AWS	Hosting provider - redirection servers
Stripe	Payment gateway

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: Arbor Education Management Infomration System (MIS)

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:	☐	☒	☐	☐	☐
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.	1.1-1.2.3, 1.2.5 – 1.5.1 2.2 - 2.2.1, 2.2.3 - 2.3.2 All of requirement 3 All of requirement 4 All of requirement 5 6.2 – 6.2.4, 6.3.2, 6.4 – 6.4.2, 6.5 – 6.5.6, All requirement 7, 8.2.3, 8.2.4, 8.2.6-8.2.8, 8.3.2-8.3.4, 8.3.8, 8.3.10-8.4.6.3 All of requirement 9 (minus 9.1.1) 10.1.2-10.7.1, 11.1.2 – 11.3.1.3, 11.4 – 11.6.1, 12.2.1-12.3.4, 12.5.1, 12.6.1 – 12.7.1, 12.10.2-12.10.7 Appendix A1, A2, A3. Due to the nature of the service, many processes ae performed entirely by Stripe therefore the above requirements are all the responsibility of third party services provders. Requirement 9 - No hard copy or electronic media containing Acocunt Data. No POI devices. Appendix A1, A2 - not a multi tenant service provider and does not use SSL/Early TLS for Card-Present POS POI Terminal Connections.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2026-07-18
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-08-17
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ 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 *(Date of Report as noted in the ROC 2026-08-17)*.

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 Arbor Education partners Limited 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 *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **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 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 *(Service Provider Company Name)* 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)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the 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

Damian Brooks

Damian Brooks (Aug 17, 2026, 9:59am)

Signature of Service Provider Executive Officer ↑	Date: 17 Aug 2026
Service Provider Executive Officer Name: Damian Brooks	Title: CTO

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:

JS Cullen

James Cullen (Aug 17, 2026, 10:03am)

Signature of Lead QSA ↑	Date: 17 Aug 2026
Lead QSA Name: James Cullen	

JS Cullen

James Cullen (Aug 17, 2026, 10:03am)

Signature of Duly Authorized Officer of QSA Company ↑	Date: 17 Aug 2026
Duly Authorized Officer Name: James Cullen	QSA Company: Cyber Security Associates limited

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 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	☐	☐	
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	☐	☐	

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/

Signable

Issuer	Cyber Security Associates Limited
Document generated	Mon, 17th Aug 2026 9:45:50 BST
Document fingerprint	76622f15d3eded0c4b352aa8865bad77

Parties involved with this document

Document processed	Party + Fingerprint
Mon, 17th Aug 2026 9:59:17 BST	Damian Brooks - Signer (8bd91ff201cdebd2a61b2023afc394a4)
Mon, 17th Aug 2026 10:03:26 BST	James Cullen - Signer (ff68aa7b258f8b75c640b777223af944)

Audit history log

Date	Action
Mon, 17th Aug 2026 9:45:50 BST	Envelope generated with fingerprint 87fe02b9d626065c9361392c9e8b8874 by james.cullen@csacyber.com (90.243.107.81)
Mon, 17th Aug 2026 9:45:50 BST	Document generated with fingerprint 76622f15d3eded0c4b352aa8865bad77 (90.243.107.81)
Mon, 17th Aug 2026 9:45:50 BST	Document generated with fingerprint e6aba09b3a8a94ad7fe7985b24cf008f (90.243.107.81)
Mon, 17th Aug 2026 9:46:46 BST	Damian Brooks has been assigned to this envelope. (90.243.107.81)
Mon, 17th Aug 2026 9:46:46 BST	James Cullen has been assigned to this envelope. (90.243.107.81)
Mon, 17th Aug 2026 9:48:49 BST	Sent the envelope to Damian Brooks (damian.brooks@arbor-education.com) for signing (90.243.107.81)
Mon, 17th Aug 2026 9:48:51 BST	Document emailed to damian.brooks@arbor-education.com
Mon, 17th Aug 2026 9:48:57 BST	Damian Brooks opened the document email. (66.249.92.132)
Mon, 17th Aug 2026 9:53:41 BST	Damian Brooks opened the document email. (66.249.93.78)
Mon, 17th Aug 2026 9:53:44 BST	Damian Brooks viewed the envelope (212.161.2.133)
Mon, 17th Aug 2026 9:53:50 BST	Damian Brooks viewed the envelope (62.252.232.8)
Mon, 17th Aug 2026 9:59:18 BST	Damian Brooks signed the envelope (212.161.2.133)
Mon, 17th Aug 2026 9:59:18 BST	Sent the envelope to James Cullen (james.cullen@csacyber.com) for signing (212.161.2.133)
Mon, 17th Aug 2026 9:59:19 BST	Document emailed to james.cullen@csacyber.com
Mon, 17th Aug 2026 9:59:40 BST	James Cullen opened the document email. (85.210.240.70)
Mon, 17th Aug 2026 10:03:05 BST	James Cullen viewed the envelope (90.243.107.81)
Mon, 17th Aug 2026 10:03:26 BST	James Cullen signed the envelope (90.243.107.81)

Mon, 17th Aug 2026 10:03:26 BST	This envelope has been signed by all parties (90.243.107.81)
Mon, 17th Aug 2026 10:03:26 BST	Signed document confirmation emailed to damian.brooks@arbor-education.com (90.243.107.81)
Mon, 17th Aug 2026 10:03:26 BST	Signed document confirmation emailed to james.cullen@csacyber.com (90.243.107.81)
Mon, 17th Aug 2026 10:03:26 BST	Signed document confirmation emails have been sent to all parties (90.243.107.81)