



# **Payment Card Industry Data Security Standard**

---

## **Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0**

Revision 2

Publication Date: August 2023



# **PCI DSS v4.0 Attestation of Compliance for Report on Compliance – Service Providers**

**Entity Name: Arbor Education Partners Limited**

**Assessment End Date: 12/08/2024**

**Date of Report as noted in the Report on Compliance: 15/08/2024**



## 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:	8th Floor, HYLO, 103-105 Bunhill Row, London, EC1Y 8LZ
Company main website:	www.arbor-education.com
Company contact name:	Damian Brooks
Company contact title:	CTO
Contact phone number:	020 3835 4025
Contact e-mail address:	Damian.brooks@arbor-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:	SureCloud Cyber Service Limited
Company mailing address:	Unit 11, Wheatstone Court, Waterwells Business Park, Gloucester, Gloucestershire. GL2 2AQ
Company website:	www.surecloudcyber.com
Lead Assessor name:	James Cullen
Assessor phone number:	0300 303 4691
Assessor e-mail address:	james.cullen@surecloudcyber.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 Information System (MIS)
------------------------------	---

Type of service(s) assessed:	
------------------------------	--

<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <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 checked="" 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 Assessment (select all that apply):**

Name of service(s) not assessed:	Not Applicable	
Type of service(s) not assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web-hosting services <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Multi-Tenant Service Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services:</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <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:		

**Part 2b. Description of Role with Payment Cards (ROC Section 2.1)**

Describe how the business stores, processes, and/or transmits account data.	<p>Arbor Education provides a Management Information System (MIS) to education organisations for the purposes of things like payroll, paying for meals and communication with parents and guardians. To use some of these features, schools are able to make payments to Arbor within the software itself.</p> <p>Additionally, the system also allows schools to take payments directly from parents and guardians for</p>
---	---



	<p>services such as school meals, uniforms, school trips and after-school clubs.</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>The Arbor MIS is hosted within Amazon Web Services (AWS).</p> <p>As a Service Provider, Arbor provides the ability for payments to its customers from parents and guardians for things like trips, uniforms and meals.</p> <p>All payments are fully outsourced and are processed via Stripe Connect. This is comprised of a client-side service, Stripe Elements, for card details to be entered directly into an iFrame provided by Stripe.</p> <p>At no point in the transaction process does Arbor Education store, process, or transmit cardholder data but they do have the ability to affect the security of the Card Data Environment (iframe).</p> <p>Upon completion of the transaction, Arbor Education receive a token to represent a confirmed payment.</p> <p>Stripe is a PCI validated service provider, compliant with the PCI-DSS evidenced by an AoC, dated 01.03.2024</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Arbor rely upon a fulfilled outsourced Iframe, served directly to the customer browser. Arbor cannot effect the storage, processing or transmission of cardholder data directly but have responsibilities for the management and security of the code repositories and the management of the virtual private cloud that the platform is hosted in.</p>



**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 Arbor platform is hosted within a virtual private cloud provided by AWS. The platform facilitates the taking of payments through Stripe Elements service, a hosted Iframe. The hosted iframe is served directly to the customer browser and card data is entered. The storage, processing and transmission of the card data is handled fully by Stripe.

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Head Office	1	London, UK



**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](http://www.pcisecuritystandards.org))—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.





**Part 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"> <li>• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Manage system components included in the 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)</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> <li>• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).</li> </ul>	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

**If Yes:**

<b>Name of Service Provider:</b>	<b>Description of Services Provided:</b>
Stripe	Payment Service Provider and IFrame provider
Amazon Web Services (AWS)	Cloud hosting provider

**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 information 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 Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 7:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>

**Justification for Approach**



<p>For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.</p>	<p>1.1-1.2.2, 1.25-1.5.1, 2.2.1, 2.2.3-2.3.2, 3.1.1-3.3.3, 3.4.2-6.2.4, 6.3.2, 6.4.1-7.3.3, 8.1.2, 8.2.3-8.2.4, 8.2.6-8.2.8, 8.3.2-8.3.4, 8.3.8-10.6.3, 10.7.2-10.7.3, 11.2-11.3.1.3, 11.4-11.6.1, 12.1.4-12.3.4, 12.5.1-12.5.2, 12.6.1-12.7.1, 12.10.2-12.10.7, - All cardholder data storage, processing and transmission is outsourced to validated third party services providers</p> <p>Appendix A - Arbor is not a shared hosting provider.                  A2 - Arbor do not utilise SSL/Early TLS                  A3 - Arbor are not a designated entity                  C - No compensating controls were used                  E - The customized approach was not used</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 1.3.2)

Date Assessment began: <i>Note: This is the first date that evidence was gathered, or observations were made.</i>		2024-07-08
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>		2024-08-12
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? If yes, for each testing activity below, indicate whether remote assessment activities were performed:		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
• Examine documentation	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Interview personnel	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Examine/observe live data	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe process being performed	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No
• Observe physical environment	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Interactive testing	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
• Other:	<input type="checkbox"/> Yes	<input checked="" 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 *(Date of Report as noted in the ROC 2024-08-15)*.

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)*:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> 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 <b>COMPLIANT</b> rating; thereby Arbor Education Partners Limited has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>								
<input type="checkbox"/>	<p><b>Non-Compliant:</b> 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 <b>NON-COMPLIANT</b> rating; thereby <i>(Service Provider Company Name)</i> has not demonstrated compliance with PCI DSS requirements.</p> <p><b>Target Date</b> for Compliance: YYYY-MM-DD</p> <p>An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.</p>								
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> 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 <b>COMPLIANT BUT WITH LEGAL EXCEPTION</b> rating; thereby <i>(Service Provider Company Name)</i> 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met						
Affected Requirement	Details of how legal constraint prevents requirement from being met								



**Part 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 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**

DocuSigned by:

*Damian Brooks*

D0402D6C2EF543D...

Signature of Service Provider Executive Officer ↑	Date: 8/16/2024
Service Provider Executive Officer Name: Damian Brooks	Title: Chief Technology Officer

**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: Observation of processes, system configurations and conducting interviews. Evidence gathering and cataloging and report writing.

DocuSigned by:

*James Cullen*

3FD09483F3B6477...

Signature of Lead QSA ↑	Date: 8/16/2024
Lead QSA Name: James Cullen	

DocuSigned by:

*James Cullen*

3FD09483F3B6477...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 8/16/2024
Duly Authorized Officer Name: James Cullen	QSA Company: SureCloud Cyber Services 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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input 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 type="checkbox"/>	<input type="checkbox"/>	

