Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

ZERTIFIKAT ★ сертификат ★ CERTIFICATE ★ CERTIFICADO ★ 證明書 ★ CERTIFICAT

besecure
Managed E-Business Security™

CERTIFICATE

BeSecure Limited

hereby certifies that it has successfully validated the

PCI DSS compliance

of

CLOUDLAYER8 LIMITED (CL8)

Falea 1, Agios Athanasios 4101, Cyprus

by means of a

PCI DSS Security Assessment [1] with report dated 28th September 2026.

Please note that this certificate is valid only in conjunction with the referenced audit reports which are part of this certificate. The scope of validation is detailed in the related Attestation of Compliance (AOC). Merchants and Service Providers are responsible for maintaining their PCI DSS compliance at any time.

BeSecure Certificate Register No.: BS2728_26C2563
Valid Until 2027-09-27

Signed by:
Andreas Lalos
CB7F29C638D4412...

[1] According to Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 4.0.1, January 2025.

Under no circumstances should this statement be construed to imply any endorsement or warranty regarding the functionality, quality, or performance of a particular product or service, and no party shall state or imply anything to the contrary. BeSecure specifically disclaims any and all representations and warranties with respect to products and services covered by the performed PCI DSS Self-Assessment Questionnaire, the PCI ASV Security Scan and the PCI DSS Security Audit, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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:	CLOUDLAYER8 LIMITED
DBA (doing business as):	CLOUDLAYER8 (CL8)
Company mailing address:	Falea 1, Agios Athanasios 4101, Cyprus
Company main website:	https://cl8.com/
Company contact name:	Michalis Stavrinou
Company contact title:	CTO
Contact phone number:	+357 25 022900
Contact e-mail address:	ms@cl8.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):	N/A
Qualified Security Assessor	
Company name:	
Company mailing address:	
Company website:	
Lead Assessor Name:	
Assessor phone number:	
Assessor e-mail address:	
Assessor certificate number:	

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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:	Colocation Services

Type of service(s) 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):		

***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.*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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:	Dedicated Servers, Disaster Recovery, Managed Services, IT Consultancy, Security Solutions, Cloud VPS

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 PCI DSS Scope is limited to Physical space (co-location) only

Part 2b. Description of Role with Payment Cards

Describe how the business stores, processes, and/or transmits account data.	CL8 does not store, process or transmit any cardholder data. CL8 provides co-location services for its customers who may process cardholder data. CL8 does not have any access to customer systems where cardholder data may exist.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	This assessment covers the provision of co-location data centre services. CL8 does not store, process or transmit any cardholder data. CL8 does not have any access to customer systems where cardholder data may exist or have any other functions or services that may impact the security of customers' account data.
Describe system components that could impact the security of account data.	Physical security controls – failure of CCTV and/or access control systems could potentially impact the physical security of customers' data (although logical

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

	security remains the full responsibility of the customers)

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.*	CL8 provides co-location physical hosting services and facilities for numerous customers; there is a strong likelihood that these customers could be processing cardholder data within these environments. For this reason, CL8 is required to align its physical security related controls to PCI DSS for the co-location site in-scope. The services offered include the provision of the physical environment, the supporting environmental services (e.g. mains power, UPS, cooling, fire detection and suppression) and physical security for the environments. Customer equipment is supplied and owned by the customer and CL8 has no logical access to this equipment
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 Center	1	Agios Athanasios, Cyprus

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

Part 2. Executive Summary *(continued)*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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)
None	N/A	N/A		

♦ 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.

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

Part 2. Executive Summary *(continued)*

© 2006—2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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:**
None	N/A

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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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: Colocation Services

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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.x - Requirements are not part of physical security for colocation providers 2.x - Requirements are not part of physical security for colocation providers 3.x - Requirements are not part of physical security for colocation providers 4.x - Requirements are not part of physical security for colocation providers 5.x - Requirements are not part of physical security for colocation providers 6.x - Requirements are not part of physical security for colocation providers 7.x - Requirements are not part of physical security for colocation providers 8.x - Requirements are not part of physical security for colocation providers 9.4.x - CL8 does not handle, store or distribute media with cardholder data in it 9.5.x - Requirements are not part of physical security for colocation providers 10.x - Requirements are not part of physical security for colocation providers 11.x - Requirements are not part of physical security for colocation providers 12.3.3 - Requirement is not part of physical security for colocation providers 12.3.4 - Requirement is not part of physical security for colocation providers 12.5.2 - Requirement is not part of physical security for colocation providers 12.8.x - There are no third-party service providers (TSPSs) 12.9.x - There are no third-party service providers (TSPSs) 12.10.7 - Requirement is not part of physical security for colocation providers Appendix A1 - CL8 is not Multi-Tenant Service Provider for colocation Appendix A2 - Requirements are not part of physical security for colocation providers
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	

© 2006—2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

Section 2: Self-Assessment Questionnaire D for Service Providers

Self-assessment completion date:	2026-09-28
Were any requirements in the SAQ unable to be met due to a legal constraint?	☐ Yes ☒ No

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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 *2026-09-28**).***

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 *CLOUDLAYER8 LIMITED* 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

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	*PCI DSS Self-Assessment Questionnaire D, Version 4.0.1,* 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

Signature of Service Provider Executive Officer ↑	*Date:* 2026-09-28
Service Provider Executive Officer Name: **Michalis Stavrinou**	*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:

Signature of Lead QSA ↑	*Date:*
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company ↑	*Date:*
Duly Authorized Officer Name:	*QSA Company:*

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:

© 2006—2024 PCI Security Standards Council, LLC. All Rights Reserved.

Docusign Envelope ID: A95990C5-082C-8A68-8385-58D164C86F6E

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	☒	☐	

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/.*

© 2006–2024 PCI Security Standards Council, LLC. All Rights Reserved.