



# Payment Card Industry (PCI) **Data Security Standard**

---

## **Attestation of Compliance for Self-Assessment Questionnaire D – Service Providers**

**For use with PCI DSS Version 3.2.1**

July 2018

## Section 1: Assessment Information

### Instructions for Submission

This document must be completed as a declaration of the results of the service provider's self-assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

### Part 1. Service Provider and Qualified Security Assessor Information

#### Part 1a. Service Provider Organization Information

Company Name:	Buuqit.com ltd	DBA (doing business as):	Channex		
Contact Name:	Evan Davies	Title:	CEO		
Telephone:	+44 7749617212	E-mail:	evan@channex.io		
Business Address:	Castell Pigyn Lodge	City:	Carmarthen		
State/Province:	Carms	Country:	United Kingdom	Zip:	SA31 2JL
URL:	https://channex.io				

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Compliance Control Ltd.				
Lead QSA Contact Name:	Evgeny Maslakov	Title:	Security Expert		
Telephone:	+7 (499) 390-20-98	E-mail:	e.maslakov@compliance-control.ru		
Business Address:	Revolucionnaya 3, office 306	City:	Volokolamsk		
State/Province:	Moscow region	Country:	Russian Federation	Zip:	143600
URL:	https://compliance-control.ru				

### Part 2. Executive Summary

#### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) assessed:	Technology solution provider				
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	<b>Managed Services (specify):</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"/> POS / 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"/> Security services		
<input type="checkbox"/> 3-D Secure Hosting Provider		
<input type="checkbox"/> Shared Hosting Provider		
<input type="checkbox"/> Other Hosting (specify):		
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" 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 checked="" 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 you feel these categories don't apply to your service, complete "Others."

If you're unsure whether a category could apply to your service, consult with the applicable payment brand.

**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 (check all that apply):**

Name of service(s) not assessed:

-

Type of service(s) not assessed:

**Hosting Provider:**

- Applications / software
- Hardware
- Infrastructure / Network
- Physical space (co-location)
- Storage
- Web
- Security services
- 3-D Secure Hosting Provider
- Shared Hosting Provider
- Other Hosting (specify):

**Managed Services (specify):**

- Systems security services
- IT support
- Physical security
- Terminal Management System
- Other services (specify):

**Payment Processing:**

- POS / card present
- Internet / e-commerce
- MOTO / Call Center
- ATM
- 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 Payment Card Business

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.	Channex.io is a connectivity platform for hotels, Channel Managers, PMS and other hotel tech vendors. The entity is a technology solution provider for e-commerce transactions. The entity provides iframe to capture card data and routes VISA, MasterCard transactions to partner service providers. The entity store PAN inside AWS RDS database in encrypted format for logging transactions information and uses tokenisation for the future transactions. Existing volume of transactions corresponds to Level 2 service providers.
Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.	No other way of being involved into the ability to impact security of CHD exist except the above.

### Part 2c. Locations

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility	Number of facilities of this type	Location(s) of facility (city, country)
<i>Example: Retail outlets</i>	3	Boston, MA, USA
Head office	1	Carmarthen, United Kingdom
Office	1	Omsk, Russian Federation

### Part 2d. Payment Applications

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
Channex PCI	1.0.0	Channex	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	N/A
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	

### Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

CDE consist of dedicated CDE segments inside AWS. All the segmentation is done with the firewalls. Only several employees can connect to the servers in the AWS via remote access. All users are connected to the CDE with remote access 2FA. All connections from partners uses strong cryptography.

Does your business use network segmentation to affect the scope of your PCI DSS environment?

*(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)*

Yes  No

### Part 2f. Third-Party Service Providers

Does your company have a relationship with a Qualified Integrator Reseller (QIR) for the purpose of the services being validated?

Yes  No

**If Yes:**

Name of QIR Company:

QIR Individual Name:

Description of services provided by QIR:

### Part 2f. Third-Party Service Providers (Continued)

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator & Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?

Yes  No

**If Yes:**

**Name of service provider:**

**Description of services provided:**

Amazon Web Services (AWS)

Hosting services

Booking.com B.V.

Online Travel Agent

Agoda

Online Travel Agent

Hostelworld

Online Travel Agent

Expedia

Online Travel Agent

master\_yield

Property Management System

protel\_turkey

Property Management System

resmaster

ermes\_hotels

resavenue

apartbook

reservation\_key

hotelier\_101

Property Management System

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

## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- Full – The requirement and all sub-requirements were assessed for that Requirement, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the SAQ.
- Partial – One or more sub-requirements of that Requirement were marked as “Not Tested” or “Not Applicable” in the SAQ.
- None – All sub-requirements of that Requirement were marked as “Not Tested” and/or “Not Applicable” in the SAQ.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the SAQ
- Reason why sub-requirement(s) were not tested or not applicable

**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.

<b>Name of Service Assessed:</b>		Technology solution provider		
PCI DSS Requirement	Details of Requirements Assessed			
	Full	Partial	None	Justification for Approach <small>(Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)</small>
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>1.4 - No mobile workstations are used to connect to the CDE.</b>
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>2.2.3 No insecure protocols are in use. 2.6 The entity is not shared hosting provider.</b>
Requirement 3:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>3.2 is not applicable because the entity do not participate in issuing services in any role. 3.4.1 - No full-disk encryption is used.</b>
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>4.1.1 - There are no wireless networks transmitting cardholder data and even connected to CDE. 4.2 - The entity does not use end-user messaging technologies to send cardholder data.</b>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>8.5.1 No remote access to customers is used.</b>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>9.6.2 and 9.6.3 - No media with CHD are sent outside the facility.</b>

Requirement 10:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<b>12.3.8-12.3.10 No remote access to CHD is allowed.</b> <b>12.9 The entity is not a shared hosting provider</b>
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>The entity is not a shared hosting provider.</b>
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<b>No insecure protocols are in use.</b>

## Section 2: Self-Assessment Questionnaire D – Service Providers

This Attestation of Compliance reflects the results of a self-assessment, which is documented in an accompanying SAQ.

The assessment documented in this attestation and in the SAQ was completed on:	29 March 2021
Have compensating controls been used to meet any requirement in the SAQ?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the SAQ identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements in the SAQ identified as being not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
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 29 March 2021.

Based on the results documented in the SAQ D noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document: **(check one)**:

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS SAQ are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby <i>Buuqit.com Ltd</i> has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS SAQ are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby (<i>Service Provide Company Name</i>) has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked “No” due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1" style="width: 100%;"> <thead> <tr> <th style="width: 35%;">Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

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

<input checked="" type="checkbox"/>	PCI DSS Self-Assessment Questionnaire D, Version 3.2.1, 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 my assessment in all material respects.
<input checked="" type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.

### Part 3a. Acknowledgement of Status (continued)

<input checked="" type="checkbox"/>	No evidence of full track data, CAV2, CVC2, CID, or CVV2 data, or PIN data storage after transaction
-------------------------------------	--

	authorization was found on ANY system reviewed during this assessment.
<input checked="" type="checkbox"/>	ASV scans are being completed by the PCI SSC Approved Scanning Vendor <i>Clone Systems, Inc. PCI cert. #4262-01-11.</i>

**Part 3b. Service Provider Attestation**

*Evan Davies*

<i>Signature of Service Provider Executive Officer</i> ↑	<i>Date:</i> <b>29 March 2021</b>
<i>Service Provider Executive Officer Name:</i> <b>Evan Davies</b>	<i>Title:</i> <b>CEO</b>

**Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)**

If a QSA was involved or assisted with this assessment, describe the role performed:	Assessor
	

<i>Signature of Duly Authorized Officer of QSA Company</i> ↑	<i>Date:</i> <b>29 March 2021</b>
<i>Duly Authorized Officer Name:</i> <b>Evgeny Maslakov</b>	<i>QSA Company:</i> <b>Compliance Control Ltd.</b>

**Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)**

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:	
---	--

## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify 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	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting 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"/>	

