



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Revision 2

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: TransactionIntel Application (TXi)

Assessment End Date: 25 Mar 2025

Date of Report as noted in the Report on Compliance: 25 Mar 2025

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:	TransactionIntel Application (TXi)
DBA (doing business as):	Not Applicable
Company mailing address:	Floor 4, Programme Bristol BS1 2LZ United Kingdom
Company main website:	www.nmi.com
Company contact name:	David Sage
Company contact title:	Vice President, Site Reliability Engineer
Contact phone number:	+1 214-471-5811
Contact e-mail address:	Daivd.sage@nmi.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:	Foregenix Ltd
Company mailing address:	1 Watts Barn Badbury Swindon Wiltshire SN4 0EU

	United Kingdom
Company website:	https://www.foregenix.com
Lead Assessor name:	Greg Marler
Assessor phone number:	+44 845 309 6232
Assessor e-mail address:	gmarler@foregenix.com
Assessor certificate number:	206-172

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:	TXi application	
Type of service(s) assessed:		
Hosting Provider: <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 <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):	Managed Services (specify): <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input checked="" type="checkbox"/> Other services (specify): Fraud scoring gateway service.	Payment Processing: <input type="checkbox"/> POS / 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 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 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: <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 <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):	Managed Services (specify): <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):	Payment Processing: <input type="checkbox"/> POS / 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:		Not Applicable

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

<p>Describe how the business stores, processes, and/or transmits account data.</p>	<p>Cardholder data (CHD) is received over HTTPS and/or SFTP via TLS v1.2 using AES 128-bit encryption. Transactions are then subsequently transmitted to the upstream processors over IPsec VPN or TLS v1.2 connections. Communication to upstream processors is dependent solely on the direction of the processors and are out of scope of this assessment.</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>Not Applicable TXi does not perform any other function that could impact the security of account data.</p>
<p>Describe system components that could impact the security of account data.</p>	<p>Firewalls, load balancers, web, application, and database servers.</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.*

Connections into the environment are web based over HTTPS using TLS v1.2 (with AES-128/256-bit encryption) or via two factor authentication using soft tokens. The CDE consists of VPCs containing load balancers, web, application, and database servers. All system OS are Windows or Linux-based and virtualized.

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)
TXi is hosted within GCP	2	US East 1 and US West 1

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:
Google Cloud Platform	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: TXi application

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 checked="" 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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" 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 checked="" 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

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

1.2.6 - Not Applicable
 Foregenix reviewed the approved network protocols and cross-referenced them with the configured network rules. They confirmed that only approved protocols were identified in the configured network rules.

1.3.3 - Not Applicable.
 Foregenix examined network diagrams, and per discussion with P-1 and P-2, there is no wireless in-scope within the assessed environment.

2.2.5 - Not Applicable.
 No insecure service or protocols are approved in the CDE. This was verified by reviewing the TXi PPS.

2.3.1 - Not Applicable.
 No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.

2.3.2 - Not Applicable.
 No wireless AP are used within the CDE. This was verified through review of the network diagrams and asset listings.

3.1.1 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD.

3.1.2 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD.

3.2.1 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.1 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.1.1 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.1.2 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.1.3 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.2 - Not Applicable.
 Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.3.3 - Not Applicable.
 TXi is not an issuer.

3.4.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.4.2 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.5.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.5.1.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.5.1.2 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.5.1.3 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.6.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.6.1.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.6.1.2 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.6.1.3 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.6.1.4 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.1 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.2 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.3 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.4 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.5 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.6 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.7 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.8 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

3.7.9 - Not Applicable.

Interview of security personnel and review of scoping documentation, network diagrams and outputs from databases confirm that TXi never stores CHD or receives SAD.

4.2.1.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2025. TXi is actively working towards achieving compliance by this deadline.

4.2.1.2 - Not Applicable.

Foregenix confirmed via interview of personnel and review of network diagrams that CHD is never transmitted over wireless networks.

4.2.2 - Not Applicable

Foregenix verified that CHD is never sent via end-user messaging.

5.2.3.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

5.3.2.1 - Not Applicable

TXi uses Qualys and CrowdStrike to run real time scans and analysis.

5.3.3 - Not Applicable

There is no removable media used in the CDE, this was verified through review of assets listing, review of data flows and interview with security personnel.

5.4.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

	<p>6.3.2 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>6.4.2 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>6.4.3 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>6.5.2 - Not Applicable Foregenix conducted comparisons between last year's system components inventory and the current one and noted no significant changes in the software versions.</p> <p>7.2.4 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>7.2.5 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>7.2.5.1 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>8.2.3 - Not Applicable Foregenix verified through interview with the Security Manager and through review of (DOC-1), it was verified that TXi does not have any access to customers' premises.</p> <p>8.2.7 - Not Applicable. Foregenix confirmed through review of business process, scoping documentation, and through interview of P-1 and P-2 that TXi does not allow any third-party accounts within the CDE.</p> <p>8.3.6 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>8.3.10 - Not Applicable. While TXi is a service provider, all accounts are considered consumer accounts.</p> <p>8.3.10.1 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>8.5.1 - Not Applicable This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>8.6.1 - Not Applicable</p>
--	--

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

8.6.2 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

8.6.3 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

9.4.1 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.1.1 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.1.2 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.2 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.3 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.4 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.5 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.5.1 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.6 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.4.7 - Not Applicable

Foregenix reviewed (DOC-1), reviewed the network diagrams and the asset inventory and confirmed TXi does not have hard-copy materials containing cardholder data.

9.5.1 - Not Applicable

Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing P-1 that there are no POI devices in the CDE.

9.5.1.1 - Not Applicable

Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing P-1 that there are no POI devices in the CDE.

9.5.1.2 - Not Applicable

Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing P-1 that there are no POI devices in the CDE.

9.5.1.2.1 - Not Applicable

Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing P-1 that there are no POI devices in the CDE.

9.5.1.3 - Not Applicable

Foregenix verified through review of network diagrams and asset inventory reviews along with interviewing P-1 that there are no POI devices in the CDE.

10.4.1.1 – Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

10.4.2.1 – Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

10.7.2 – Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

11.3.1.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

11.3.1.2 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

11.3.1.3 - Not Applicable

While interviewing security personnel, it was identified that the internal and external scans are run frequently and scheduled with the reports being reviewed. The scans are unattended and therefore, based on the change management process, do not require a change to be logged for vulnerability scans. Change controls are logged for all changes and remediation required based on the review of the vulnerability scan reports. There were no significant changes to CDE identified within the last 12 months.

11.3.2.1 - Not Applicable

While interviewing security personnel, it was identified that the internal and external scans are run frequently and scheduled with the reports being reviewed. The scans are unattended and therefore, based on the change management process, do not require a change to be logged for vulnerability scans.

Change controls are logged for all changes and remediation required based on the review of the vulnerability scan reports. There were no significant changes to CDE identified within the last 12 months.

11.4.7 – Not Applicable

TXi is not a multi-tenant service provider.

11.5.1.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

11.6.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.3.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline

12.3.2 - Not Applicable

Foregenix validated all the requirements of this report and found no requirements using customized approach to achieve compliance.

12.3.3 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.3.4 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.5.2.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.5.3 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.6.2 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.6.3.1 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.6.3.2 - Not Applicable

This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.

12.10.4.1 - Not Applicable

	<p>This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>12.10.7 - Not Applicable</p> <p>This requirement is considered a best practice until 31 Mar 2024. TXi is actively working towards achieving compliance by this deadline.</p> <p>A1.1.1 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.1.2 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.1.3 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.1.4 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.2.1 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.2.2 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A1.2.3 - Not Applicable</p> <p>TXi does not perform shared hosting provider functions.</p> <p>A2.1.1 - Not Applicable</p> <p>TXi does not have POI terminals.</p> <p>A2.1.2 - Not Applicable</p> <p>TXi does not have POI terminals.</p> <p>A2.1.3 - Not Applicable</p> <p>TXi does not have POI terminals.</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>	17 Mar 2025
Date Assessment ended: <i>Note: This is the last date that evidence was gathered, or observations were made.</i>	25 Mar 2025
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?	<input checked="" type="checkbox"/> Yes <input 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 25 Mar 2025)*.

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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby TransactionIntel Application (TXi) 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 TransactionIntel Application (TXi) has not demonstrated compliance with PCI DSS requirements.

Target Date for Compliance:

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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby TransactionIntel Application (TXi) 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 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 4.0.1 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



Signature of Service Provider Executive Officer ↑	Date: 25 Mar 2025
Service Provider Executive Officer Name: David Sage	Title: Vice President, Site Reliability Engineer

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: The QSA reviewed the scope of the assessment, reviewed documentation, interviewed responsible personnel, and validated all applicable system component configurations and processes.



Signature of Lead QSA ↑	Date: 25 Mar 2025
Lead QSA Name: Greg Marler	



Signature of Duly Authorized Officer of QSA Company ↑	Date: 25 Mar 2025
Duly Authorized Officer Name: Dan Farr	QSA Company: Foregenix Ltd.

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

ISA(s) performed testing procedures.

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:

ISA(s) provided other assistance.

If selected, describe all role(s) performed: Not Applicable

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"/>	

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/