Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046



Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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

Entity Name: Argo IT Tecnologia S/A

Date of Report as noted in the Report on Compliance: 07/31/2026

Date Assessment Ended: 07/31/2026

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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:	Argo IT Tecnologia S/A
DBA (doing business as):	Argo Solutions
Company mailing address:	Alameda Santos, 1976 – 11th Floor – 01418-102 – Cerqueira César – São Paulo – SP – Brazil
Company main website:	https://useargo.com/
Company contact name:	Aline Bueno
Company contact title:	CEO
Contact phone number:	+55 11 94558-9644
Contact e-mail address:	aline.bueno@useargo.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:	Cipher S.A
Company mailing address:	1435, Ermano Marchetti Avenue, 8th floor, Lapa de Baixo, São Paulo, SP, Zip Code 04717-004, Brazil
Company website:	https://cipher.com
Lead Assessor name:	Janaina Devus Creazzo
Assessor phone number:	+55 11 4501-6600
Assessor e-mail address:	jcreazzo@cipher.com

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

Assessor certificate number:	#056-017

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:	Argo Travel Management Platform

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): Not Applicable		

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.

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:	Argo Travel Management Platform

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:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	Argo Solutions operates a travel management application that connects travel agencies and corporate clients for booking services such as hotels, flights, car rentals, and ground transportation. Account data is stored in cloud-based infrastructure hosted on Microsoft Azure, using strong encryption mechanisms managed through Azure HSM Key Vault. Sensitive authentication data is not stored alongside other cardholder data and is instead maintained in a separate HSM-based environment located in a different datacenter, ensuring secure data segregation. During storage and

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

	processing, encryption and data masking are applied to protect sensitive information. Data transmission is secured using HTTPS with TLS 1.2 protocol, ensuring confidentiality and integrity of account data in transit. Access to data is strictly controlled and monitored.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Argo Solutions stores and transmits cardholder data as part of its travel management platform. All data transmissions are secured using industry-standard encryption protocols and digital certificates. Stored data is encrypted using strong cryptographic controls, and sensitive authentication data is segregated and protected in a dedicated HSM environment. As a result, Argo has a direct impact on the security of its customers' account data through its infrastructure, data handling practices, and security controls.
Describe system components that could impact the security of account data.	Argo Solutions operates its environment entirely in the Microsoft Azure cloud, where multiple system components contribute to the protection and potential impact on the security of account data. These include web servers, database servers, Active Directory and infrastructure servers, as well as load balancers that manage traffic distribution. Network segmentation and firewall rules are configured both within Azure and through the Azion Web Application Firewall (WAF), ensuring layered perimeter protection. Security is further reinforced by SentinelOne for endpoint protection, Rapid7 for centralized log management and threat detection (SIEM), and Azure HSM and dedicated HSM servers for cryptographic operations and secure key storage. These components collectively support the confidentiality, integrity, and availability of cardholder data across the environment.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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.*	Argo Solutions maintains two environments that store and transmit cardholder data: one hosted in Microsoft Azure and another dedicated HSM environment located in a separate datacenter. The Azure environment includes critical system components such as web servers, databases, infrastructure servers, and the Argo OBT application developed in-house. The HSM environment is used exclusively for secure storage of sensitive authentication data. Connections into and out of the CDE are protected using secure protocol (TLS 1.2), and the environment is supported by security components including Azion WAF, SentinelOne EDR, Rapid7 SIEM, and Azure-native firewall and network controls. These components collectively ensure the confidentiality, integrity, and availability of account data.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☒ Yes ☐ No

Part 2d. In-Scope Locations/Facilities (ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Corporate Office	01	São Paulo,SP - Brazil
Azure	02	East 2 and South Brazil

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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:
Azure	Cloud Service Provider

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

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: Argo Travel Management Platform

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☒	☐	☐	☐
Requirement 2:	☒	☒	☐	☐	☐
Requirement 3:	☒	☒	☐	☐	☐
Requirement 4:	☒	☒	☐	☐	☐
Requirement 5:	☒	☒	☐	☐	☐
Requirement 6:	☒	☒	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐
Requirement 8:	☒	☒	☐	☐	☐
Requirement 9:	☒	☒	☐	☐	☐
Requirement 10:	☒	☒	☐	☐	☐
Requirement 11:	☒	☒	☐	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☒	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.3.3, 2.3.1, 2.3.2, 4.2.1.2 - Not applicable, as they do not have wireless networks in scope. 3.5.1.2, 3.5.1.3 - Not applicable as it is applied to encryption on the server. 3.3.1.3 - Not applicable, they do not work with card passwords. 3.3.1.1 - Not applicable, they do not work with magnetic stripes. 3.3.3 - does not apply to ARGO, as the organization does not act as an issuer nor provides services related to the issuance of cards. 3.7.9 - This does not apply to ARGO, as the organization does not share cryptographic keys with third parties. All keys used for account data encryption are stored and managed internally in hardware security modules (HSM). 2.2.5 - They do not use insecure protocols, services, or daemons. 4.2.2 - Not applicable as they do not have Messaging services. 5.2.3, 5.2.3.1 - They do not have systems without the risk of malware. 5.3.2.1 - Not applicable, as they have behavioral scans and real-time monitoring using SentinelOne. 6.4.1, 8.3.10, 10.7.1 - The requirement was discontinued since April 1, 2025. 6.4.3, 11.6.1 - They do not have Cashout payment pages, as they are processed by the providers, they only send the information to the company that will process the payment. 8.2.3, 8.2.7 - They do not have third parties and service providers who make this access. 8.6.2 - Interactive logins cannot be performed on system accounts. 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6, 9.4.7 - Not applicable as they do not have physical media of the card data. 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3 - Not applicable, They do not have POI devices. 10.4.2, 10.4.2.1 - Not applicable, all audit records are already captured. 11.4.7 - The requirement does not apply to ARGO, as the organization does not operate as a multi tenant service provider nor does it offer services in cloud or shared environments with external clients.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2026-06-22
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-07-31
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC 2026-07-31)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☐ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby Argo IT Tecnologia S/A has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Docusign Envelope ID: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

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

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Assinado por:
9E3FC03CD6C74B2...

Signature of Service Provider Executive Officer ↑	Date: 2026-07-31
Service Provider Executive Officer Name: Aline Bueno	Title: Chief Executive Officer (CEO)

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:

Assinado por:
Janaina Devus
BF67742607034AD...

Signature of Lead QSA ↑	Date: 2026-07-31
Lead QSA Name: Janaína Devus Creazzo	

Assinado por:
Paulo Poi
845AD8ECDFF9401...

Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-07-31
Duly Authorized Officer Name: Paulo Rogerio de Aguiar Poi	QSA Company: Cipher S/A

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: CCC5CAB1-B32B-8C3A-80BF-65FD71C1C046

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.