COMPLIANCE CONTROL

CERTIFICATE OF PCI DSS COMPLIANCE

This is confirmation that the Entity:

CJSC «Markazı Tekhnologiyahoi Muosir»

Has been assessed by Compliance Control Ltd. and was found to be compliant with
Payment Card Industry Data Security Standards 4.0.1.
It was confirmed by annual security assessment performed by QSAs of Compliance Control Ltd.

Certificate is valid till:	**30 January 2026**
PCI DSS version:	**4.0.1**
Certificate No.	**5TBC-3RWE-1ZQK**

Issue date:
31 January 2025

Ivan Tverdokhlebov
QSA

Signature

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

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

Entity Name: CJSC "Markazi Tekhnologiyahoi Muosir"

Date of Report as noted in the Report on Compliance: 31st January 2025

Date Assessment Ended: 31st January 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:	CJSC "Markazi Tekhnologiyahoi Muosir"
DBA (doing business as):	MTM
Company mailing address:	37/1a Bokhtar str., Dushanbe, Tajikistan, 734000
Company main website:	https://mtm.tj/
Company contact name:	Olim Karimov
Company contact title:	Head of Information Security Department
Contact phone number:	+992880009099
Contact e-mail address:	o.karimov@mtm.tj
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):	N/A
Qualified Security Assessor	
Company name:	Compliance Control Ltd.
Company mailing address:	Punane tn. 16/1-414, Tallinn, Harju, Estonia, 13619
Company website:	https://www.compliance-control.eu
Lead Assessor name:	Yevhen Koshelkov
Assessor phone number:	+380633853243
Assessor e-mail address:	ykoshelkov@compliance-control.team
Assessor certificate number:	204-914

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:	MTM Payment Processing	
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☒ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☒ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☒ POI / card present ☒ Internet / e-commerce ☐ MOTO / Call Center ☒ ATM ☐ Other processing (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.*

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:		
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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:		

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.	The main direction of CJSC “Markazi Tekhnologiyahoi Muosir” is the implementation of multiple projects of Local cards and electronic wallets, which simultaneously participate in the domestic program for unifying acquiring networks called “Imcon”. The main priorities of these projects for issuing Local cards are Electronic Wallets, virtual cards and modern Internet technologies, making payments and transferring funds in addition to traditional banking products and services. CJSC "Markazi Technologyhoi Muosir" is the only third-party Processing center in the Republic of Tajikistan.

	Current transaction amount for CNP and CP operations is more than 1 mln. for last year.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	Currently, the entity utilizes BPC Payments Services SmartVista 2.2.25.R-ACS approved by VISA, Reference No. 3DS_LOA_ACS_BPBT_020200_00679 / 2.2.25.R-3DSS approved by VISA, Reference No. 3DS_LOA_SER_BPBT_020200_00676, a complex solution that ensures secure payment cards usage in Internet. The solution supports inter-host interaction with issuers and acquirers, as well as with international payment systems.
Describe system components that could impact the security of account data.	Internal hosted components: - Firewalls / switches (Watchguard, Huawei); - Oracle databases; - Oracle virtualization platform; - FIM / SIEM (OSSEC); - Modsecurity WAF; - DLP Staffcop; - Docker; - Windows, Ubuntu, Oracle Linux OS; - Nmap vulnerability scanner; - Kaspersky and ClamAV Antiviruses; - etc.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The scope of this assessment includes: • main payment and infrastructure systems - processing system SmartVista, Oracle virtual infrastructure, security systems, and components of these systems; - hypervisors, web servers, application servers, database servers, authentication servers, time servers (NTP), firewalls, switches, routers, network security devices (IPS); • Computing network of MTM, segmentation of the computer network and external network connections; • information security management processes required by PCI DSS; • personnel who has access to the information environment and / or data on payment card holders: administrators, payment system operators, security staff.
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*
Head office and own data center	1	37/1a Bokhtar str, Business Center "Bokhtar" building, office #906, Dushanbe, Tajikistan

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
BPC SmartVista FE	2.2.10	PA-DSS v2.0	13-02.00203.002	28th October 2016

* 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:
Payment-guide	POS terminals maintenance
International processing systems LLC	E-com merchant service

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: MTM Payment Processing

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

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.6 - No insecure services, protocols or ports are allowed and used. 1.3.3 - There are no wireless networks in the provider's cardholder data environment. 1.5.1 - Computing devices connected to both untrusted networks and CDE are not used 2.2.5 - No insecure services, protocols and daemons are used. 2.3 - There are no wireless environments connected to cardholder data environment or transmitting cardholder data. 3.3.2 - SAD is not stored prior to completion of authorization 3.3.3 - The entity does not store sensitive authentication data. 3.5.1.2 - Disk encryption is not used. 3.7.9 - The enity is not a service provider that shares keys with their customers for transmission or storage of cardholder data. 4.2.1.2 - There are no wireless networks transmitting cardholder data and even connected to cardholder data environment. 4.2.2 - The entity does not use end-user messaging technologies to send unprotected cardholder data. 5.2.3 - The entity considers all systems may be affected by malicious software. 6.2 - The entity uses payment application from its vendor BPC and does not use internally developed payment applications. Therefore, software development processes are not in the scope of this PCI DSS assessment. 6.5.2 - No significant change occurred within the past 12 month. 8.2.3 - The organization does not use remote access to customer premises. 8.2.7 - No active vendor accounts for remote access 8.3.10 - The organization does not store customer passwords to access cardholder data 9.4.3 and 9.4.4 - No media with CHD are sent outside the facility. 9.4.6 - No hard-copy materials are used. 9.5.1 - The organization bears no responsibility for devices that capture payment card data via direct physical interaction. 5.4.1, 6.4.3, 11.6.1, 12.10.5, 12.9.2 - These requirements are the best practice until 31 March 2025. 11.4.7, A1 - The organization is not a Multi-Tenant Service Provider. 12.3.2 -The entity doesn't use customized control to meet PCI DSS requirements. A2 - The organization does not use SSL / early TLS.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

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.*	9th October 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	31st January 2025
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

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 31st January 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 In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby CJSC "Markazi Tekhnologiyahoi Muosir" 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

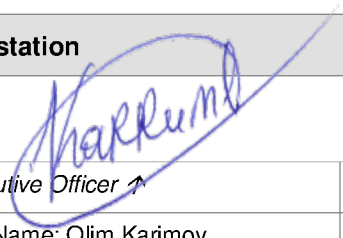
Part 3. PCI DSS Validation *(continued)*

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.

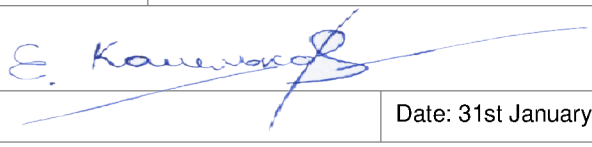
Part 3b. Service Provider Attestation



Signature of Service Provider Executive Officer ↗	Date: 31st January 2025
Service Provider Executive Officer Name: Olim Karimov	Title: Head of Information Security Department

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: 31st January 2025
Lead QSA Name: Yevhen Koshelkov	

Signature of Duly Authorized Officer of QSA Company ↗	Date: 31st January 2025-DD
Duly Authorized Officer Name: Mykhailo Mahun	QSA Company: Compliance Control Ltd.

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

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

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

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

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☒	☐	
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/