Technical Compliance sheet

LOT No. 01 Transaction Monitoring System		
Sr	Features	Compliance status (Yes/NO)
1	The solution must include but not limited to • Automated Transactions Monitoring System • bundled Know your Customer (KYC) Module/Application	
2	• The solution should be highly scalable and offer a modern service-oriented architecture. • Solution should have message queuing functionality built in • Solution should both horizontally and vertically scalable • Solution should be independent of physical servers and can be deployed in virtual environment.	
3	System Should have capability that all sensitive data must be encrypted both in transit and at rest using strong encryption algorithms.	
4	System should have capability of Role-Based Access Control (RBAC) to restrict access to the system, based on users' roles and responsibilities.	
5	System should Log all system activities, including user logins, data accesses, configuration changes, and transaction monitoring activities.	
6	System should have capability to integrate with elastic security SIEM solution to centralize security log management, correlation, and analysis for proactive threat detection.	
7	Vendor shall perform and share the Vulnerability Assessment and Pen Testing report of system in scope, along with remediation status before go live.	
8	Should be support industry known multifactor authentication technologies/protocol (if required)	
9	Solution should support SSL / TLS implementation with Client authentication certificates.	
9	Bidder should provide any updates released by bidder in the platform without any cost.	
10	During installation and testing onsite, provide detailed instruction to IT on the maintenance of the application software, to include system recovery and security, Setup Live, Disaster Recovery, Development & QA instances of the application software separately.	
11	Bidder should provide detailed training to ZTBL nominated Project Implementation Team (PIT), 10 to 15 users, before go live.	
12	Solution should support API-based integration with the Bank’s and SBP systems, with no limitation on development of required interfaces/integrations.	

13	The system shall offer a large set of predefined rules that can be combined to create a maximum possible number of scenarios with varying complexities.	
14	Compliance features: Customer Card and Account Card modules to allow users to capture specific details such as: Account Controlling Persons and Beneficial Owners, Directors and Signatories of Corporates and other Legal Representative and Shareholders. All mentioned parties have the possibility to be flagged as PEP or Not PEP.	
15	User can track any changes in customer's data loaded from back office to the Profiling application. The type of data to monitor can be dynamically selected.	
16	Integration with another Transaction Data Repository product and shall allow users to search for any information related to customers in the application. Moreover, using the Rule Builder user can build new scenarios to monitor those loaded messages.	
17	To ensure full compliance with the latest national and international laws and regulations, complies with SBP AML/CFT/CPF Regulations, Data Protection rules etc	
19	Allows the loading and the creation of counterparty lists to better monitor certain counterparties especially when they are not customers in the bank. This includes displaying connections between existing customers and any counterparties defined in the registry, defining scenarios to monitor transactions coming from or going to specific counterparties through the rule builder, and screening Counterparties against defined black lists.	
20	System should support identification, monitoring, and configurable alert generation for virtual asset-related transactions, payment patterns, VASP-specific risks, typologies and red flags, with separate classification and risk-rating of VASPs and related customers / entities from conventional customers.	
21	System should support detection of structuring, layering, rapid movement of funds, mule account behavior, and unusual transaction velocity related to VASPs and their customers.	
22	System should provide dashboards and MIS reporting for Virtual Asset Service Provider (VASP) related alerts.	
23	System should generate automated alerts where transactions are conducted between Client Money Accounts (CMAs) and other operational or business accounts of Virtual Asset Service Providers (VASPs), in accordance with the monitoring and control requirements	

	prescribed under SBP BPRD Circular Letter No. 10 of 2026 dated April 14, 2026.	
24	System should support future regulatory changes related to Virtual Asset Service Providers (VASPs) VASP and regulatory requirements.	
25	System should be capable of generating automated alerts based on typologies/scenarios/red flags related to Home Remittances transactions and Locker Operations transactions.	
	KYC Application	
i.	KYC Form User can create a new KYC form for any of Physical, Legal and Financial Institution customers. The KYC form enables user to enter all information related to the customer, to help him/her evaluate the customer's risk.	
ii.	KYC Form Builder: The form builder to enable users to create dynamic and customized forms for KYC by creating new blocks, adding their own new fields with the different options of data types, mandatory/optional, visible and not visible, and moving fields around. In addition to linking those fields to the risk scoring of KYC easily.	
iii.	KYC Validity Period: Validity period for KYC forms can be specified in Months, to maintain more accurate data for customers.	
iv.	Notification Emails: For a flawless monitoring, sending emails is activated on API instantly when a new KYC record is inserted to specific emails.	
v.	Support four eyes principal: can send any newly created or amended KYC form to another person for approval/review, can assign different statuses to the form according to the certain approval processes the KYC form will go through.	
vi.	Compliance with CDD KYC: KYC forms allow users to capture specific details such as: Account Controlling Persons and Beneficial Owners, Directors and Signatories of Corporates and other Legal Representative and Shareholders. All mentioned parties have the possibility to be flagged as PEP or Not PEP.	
vii.	Identify a risk score for each Customer: The System shall help the bank automatically calculate a risk score for each Customer by building risk criteria and weighing each risk element. Risk scoring also allows the sorting of alerts according to a customer's risk level. The formula and structure shall have been designed to comply with the FATF recommendation of the customer risk assessment and of SBP AML/CFT/CPF Regulations and other laws	

viii.	KYC Attachment: The user can upload the required attachments related to a certain customer(s). This can be a scanned passport, contract, identification document or any other possible electronic document.	
ix.	Configure On boarding acceptance criteria: KYC enables users to define the criteria upon which a certain customer will be accepted or rejected. This will assign each KYC an Auto Status which will prevent any internal fraud attempts. Manually approved KYC forms that should not be approved as per the acceptance criteria will be detected through the un-editable auto status value.	
x.	Screening against Blacklists: Upon creating or updating the KYC form, system automatically scan the Customer Name, Representative Name and Beneficial Owner Name against the black lists defined in the application.	
xi.	Configuration of KYC Forms Validity Per Customer Risk: Users can specify the validity period for KYC forms based on customers' risk. This will enable the bank to maintain up-to-date KYC forms and improve the due-diligence level done for their customers. Reports can be generated to list customers with KYC forms that are about to expire.	
xii.	KYC solution shall be able to be integrated with bank core systems. Configurability: Bank Users can change, add duplicate, and delete configurations, parameters, risk score, and scenarios, etc. by their own without additional consultancy fees.	
xiii.	System Should maintain beneficial ownership (UBO) identification and verification for Virtual Assets Service Providers (VASP) related entities.	
xiv.	System should have support digital KYC onboarding workflow for VASPs and their customers with full audit trail.	
xv.	System should have support for document management and e-KYC repository with version control and retention.	

Note:- Please clearly indicate compliant/non complaint (Yes/NO) against each without remarks. The partial compliance with or without remarks against any item will be treated as non-compliance. **All the technical requirements are mandatory, non-compliant/partial compliant against any item will be declared as Technically Non-Compliant Bidder.**