

**FINCA Kyrgyzstan**

**Compliance/AML system**

**Request for Proposal**

**July, 2024**

ALL MATERIAL IN THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY TO FINCA IMPACT FINANCE. AND MAY NOT BE USED BY ANY (PARTY OR PERSON) FOR ANY REASON OTHER THAN TO SUBMIT AN INFORMATIONAL RESPONSE TO FINCA IMPACT FINANCE.

**Contents**

[Confidential and proprietary 4](#_Toc170929891)

[1.1 Profile of FINCA Kyrgyzstan 4](#_Toc170929892)

[1.2. FINCA Kyrgyzstan RFP 4](#_Toc170929893)

[1.2.1.1 Products and Services 5](#_Toc170929894)

[2. Background and scope 6](#_Toc170929895)

[2.1 RFP process schedule 7](#_Toc170929896)

[3. Requirements overview 8](#_Toc170929897)

[3.1 Compliance and Anti-Money Laundering Solution Business Requirements 8](#_Toc170929898)

[3.1.1 Products and services 8](#_Toc170929899)

[3.2 Technical requirements 14](#_Toc170929900)

[4. Response terms and conditions 18](#_Toc170929901)

[5. Contents of proposal 19](#_Toc170929902)

[5.1 Appendix A: Vendor’s response template 19](#_Toc170929903)

[5.2 Appendix B: Business Requirements 20](#_Toc170929904)

[5.3 Appendix C: Total cost of ownership template 20](#_Toc170929905)

[5.3.1. License and support 20](#_Toc170929906)

[5.3.2 Implementation 20](#_Toc170929907)

[5.4 Additional documentation 21](#_Toc170929908)

[5.4.1 Team resumes 21](#_Toc170929909)

[5.4.2 Project organizational chart 21](#_Toc170929910)

[5.4.3 Subcontracting 21](#_Toc170929911)

[5.4.4 References 21](#_Toc170929912)

[6. Selection criteria 22](#_Toc170929913)

[6.1 Evaluation of responses 22](#_Toc170929914)

[6.2 Vendor demonstrations and score validation 23](#_Toc170929915)

[6.3 Reference checks 23](#_Toc170929916)

[6.4 Vendor selection 23](#_Toc170929917)

[7. Communication and Q&A protocol 23](#_Toc170929918)

[7.1 Written inquiries 23](#_Toc170929919)

[7.2 Vendor demonstrations 23](#_Toc170929920)

[8. Next Steps 24](#_Toc170929921)

# Confidential and proprietary

This Request for Proposal (“RFP”) has been prepared by FINCA Kyrgyzstan (“FINCA” or “we”) and is being given to you (“Vendor”) to provide you with an opportunity to participate in the System selection process, in consideration of your agreement to treat it as confidential.

The information enclosed in this document is proprietary to FINCA. The release and use by you in preparation of a response to the RFP do not convey any ownership to any party by FINCA’s disclosure of this information.

By accepting this document, you agree that you will treat this information as confidential and you will not use it for any other purpose than to prepare the requested response. This information may not be disclosed to others without the express written consent of an authorized representative of FINCA.

You will return this document, and all copies you have made of it, to FINCA upon FINCA’s request or if you should decline to submit responses. You will also return any additional hard copies of this document and delete any electronic copies.

# 1.1 Profile of FINCA Kyrgyzstan

The mission of FINCA is to alleviate poverty through lasting solutions that help people build assets, create jobs, and raise their standard of living.

For more than 29 years, FINCA Bank has been operating in Kyrgyzstan. Over these 29 years, we have gone from a simple business lending program to a full-fledged Bank with a wide range of banking services and products. We are in the TOP-10 of the most successful and largest banks in Kyrgyzstan.

Today we are a modern Bank with more than 1200 employees who serve more than 250 thousand clients in more than 90 offices throughout Kyrgyzstan. We have ambitious plans ahead! We will also adhere to our mission, support entrepreneurs, implement socially significant projects and contribute to the development of society and the economy of Kyrgyzstan.

FINCA Bank is actively working to improve and develop existing products and services. Our Bank aims to develop and implement new digital banking technologies that will allow our clients to use our services of the highest quality conveniently and remotely.

## 1.2. FINCA Kyrgyzstan RFP

FINCA Bank Kyrgyzstan is inviting proposals from qualified vendors to provide a comprehensive Compliance and Anti-Money Laundering (AML) off-the-shelf solution. The selected vendor will be responsible for delivering and implementing two key modules: Customer Due Diligence and Transaction Monitoring & Anti-Money Laundering.

### 1.2.1.1 Products and Services

By offering credit products to micro-entrepreneurs, FINCA Kyrgyzstan provides its customers with a sustainable way to build their business and ultimately improve the quality of life for themselves and their families.

|  |  |
| --- | --- |
| Loans | * **Loans for individuals** * Consumer loans * Loans for education * Salary loans * Overdrafts * Loans for women * Group loans for business development * Agricultural loans * **Loans for legal entities** * Loans for small and medium business owners * Loans for private entrepreneurs * Agricultural loans |
| Deposits | * **Deposits for individuals** * Fixed term deposits * Savings deposits * Retirement deposits * Women's deposits * Child deposits * **Deposits for legal entities** * Fixed deposits   Savings deposits |
| Services | * Demand accounts * Settlement and cash services * Money transfers * Settlement accounts * Bank guarantees * Currency exchange * Internet banking * Mobile banking * Remote identification |

# 2. Background and scope

1. Purpose:

Implementation of Compliance/AML solution is a project aimed to automate day to day manual compliance activities. We are looking for the system that meets our requirements and covers our existing business processes and workflows which shall be present in the following solution modules and functions:

1. Functional Requirements (detailed information in section 3 «Requirements overview»):

Module 1: Customer Due Diligence: Watchlist Screening, Name Screening, CRM Monitoring, Compliance Management, User Maintenance and Security, Onboarding process requirements, Requirements for Risk Profiling.

Module 2: Transaction Monitoring & Anti-Money Laundering: AML Rule Engine (detection methodologies), Alerts Management, Scenarios Monitoring, User Maintenance and Security, Alert Generation Setup, Requirements for Clients’ ongoing monitoring, Requirements for Ongoing Monitoring of Transactions (Local and International), Case management, Requirements for Reporting, Requirements for Audit trail and other requirements.

1. Integration:
   1. Integrate with existing banking Systems, such as the Core Banking System (CBS).
   2. Integrate with third-party services and APIs, including payment gateways and other relevant financial platforms.
2. Implementation Plan: The implementation plan should include the following key components:

* Project kickoff and initiation.
* System configuration and customization.
* Integration with existing systems.
* User training and documentation.
* User acceptance testing (UAT).
* Deployment and Go-Live.

1. Deliverables: Upon successful implementation, the vendor is expected to deliver the following:

* Fully configured and operational Customer Due Diligence and Transaction Monitoring & AML modules.
* Training of compliance, IT staff.
* Training materials and documentation for end-users.
* A comprehensive report on the testing, validation of the solution and supporting.

1. Timeline: The project is expected to be completed within 6 months from the project kickoff date.
2. Support and Maintenance: The vendor is expected to provide ongoing support and maintenance services post-implementation, including updates, patches, and troubleshooting. Response time for the support reaction in case of downtime shall not exceed the reasonable time set out in the Contract.
3. Budget: The proposed budget for the entire project, including licensing, implementation, and ongoing support/maintenance, should be detailed in the proposal.

## 2.1 RFP process schedule

The following is the expected timetable for distribution and submission of RFP responses.

| ***Event*** | ***Date*** |
| --- | --- |
| RFP announcement and distribution to vendors | July 10, 2024 |
| Vendor questions due date | July 25, 2024 |
| RFP Responses due date | August 12, 2024 |
| Confirmation of vendors / Systems selected for demo due date | September 3, 2024 |
| Vendor demo sessions due date | September 19, 2024 |
| Evaluation of proposals due date | October 3, 2024 |
| Selection and approvals due date | November 13, 2024 |

FINCA reserves a right to modify above mentioned planned activities as well as proposed timeframes at any time.

All responses to the RFP are due by 6pm, GMT +6 on August 12th 2024. The preferred method of submission is via email as mentioned in section 8 of this RFP.

FINCA has no obligation to disclose Vendors’ identities to other Vendors.

# 3. Requirements overview

The following section contains an overview of business requirements and descripton of requirements for customization and implementation process that FINCA expect from the Compliance and Anti-Money Laundering Solution and vendor.

## 3.1 Compliance and Anti-Money Laundering Solution Business Requirements

Compliance and Anti-Money Laundering Solution is a unique project that requires the establishment of core capabilities to operate in the financial services industry and integrate those capabilities into an efficient global platform. Compliance and Anti-Money Laundering Solution should possess functional and flexible features that enable FINCA to offer a wide range of banking services to its customers. The required Compliance and Anti-Money Laundering Solution should comply with country-specific regulations issued by the respective regulatory bodies. Compliance and Anti-Money Laundering Solution should have the capability to integrate with external Systems, including interfaces provided by local regulatory authorities and various agencies.

### 3.1.1 Products and services

Compliance and Anti-Money Laundering Solution must have robust functionality to support current operational needs as well as future planned processes and activities. The list of functionalities provided by the vendor in the Compliance and Anti-Money Laundering software should cover the following areas. The same list is attached in Annex B, which is mandatory for inclusion in the vendor's proposal, along with appropriate compliance and comments.

The above overview presents the business requirements and functional capabilities of the Compliance and Anti-Money Laundering Solution in the FINCA project. These requirements define the need for a flexible and functional solution that can support current operational needs and comply with regulatory requirements and external System integration.

**II. Business Objectives:**

**Compliance Assurance:**

* Ensure adherence to international and Kyrgyzstan regulatory requirements, including UN, OFAC, EU, UK sanctions, and Kyrgyzstan national lists.

**Risk Mitigation:**

* Identify and mitigate the risk of money laundering and fraudulent activities through advanced detection methodologies.

**Efficient Customer Due Diligence:**

* Streamline the customer due diligence process for account opening and ongoing monitoring.

**Alert Management and Investigation:**

* Promptly manage and investigate alerts generated by the system to ensure compliance with regulations.

**User Access Control:**

* Implement robust user access controls to safeguard sensitive information and prevent unauthorized access.

**Integration with Existing Systems:**

* Seamless integration with the Core Banking System, с Oz Liveness Oz Biometry web SDK (by Oz forensics), Pay logic, CRM, DFA, Mobile Banking/Internet Banking and any other third-party systems to ensure data consistency.

**Customizable Scenarios:**

* Enable the creation and modification of compliance scenarios to address evolving business needs.

**Real-time Monitoring:**

* Provide real-time monitoring capabilities for Customer Relationship Management (CRM) during account opening.

**III. Functional Requirements:**

**Module 1: Customer Due Diligence:**

* + 1. **Watchlist Screening:**
* Real-time screening against sanctions lists of EU, OFAC, UN, UK, Kyrgyzstan national lists any list of clients that FINCA considers as non-acceptable or should be monitored (Internal black lists), the list of high-risk countries.
* Integration with customer screening platform to check against sanctions lists with automatic/manual list update mechanisms. The system shall support import and synchronization from web sources (HTTPS, SFTP) including support of formats XML, TXT, CSV etc.
* The system shall have the audit trail, logs for lists updates, history on deleted persons/entities, decisions-made etc.
  + 1. **Name Screening:**
* Black-listers checking with algorithm-based matching criteria for individual and bulk screening.
* Possibility to set different types of response (full blocking for certain lists and just notification for others)
  + 1. **CRM Monitoring:**
* Real-time monitoring of CRM during account opening.
* Multi-supervision functionality.
  + 1. **Compliance Management:**
* Alert assignment for single and bulk alerts.
* Investigation workflow and Compliance Certificate generation.
* Attachment of evidence for compliance documentation.
  + 1. **User Maintenance and Security:**
* Multi-level Role Management.
* Integration and mapping with the Core Banking System, с Oz Liveness Oz Biometry web SDK (by Oz forensics), Pay logic, CRM, DFA, Mobile Banking/Internet Banking, FINCA Global AML and any 3rd party systems.
  + 1. **Onboarding process requirements:**
* The system shall be able to perform real-time screening of customers during onboarding process against watch list, block onboarding process before compliance officer’s decision-making. For high-risk customers system shall be able to support escalation process to senior management.
* The system shall be able to screen proxies, UBOs, authorized entities.
* The system shall be able to perform real-time screening according to the pre-defines scenarios.
* The system shall be able according to pre-defines scenarios to escalate high risk customers for approval from front-office to compliance and further to senior management.
* Customer approval/postpone/rejection decisions shall be traceable and shall have an option to document justification.
* Configuration and update of KYC forms and risk profiling of customers, and to allow the customization of KYC forms per subsidiary.
* The system shall be able to perform real-time screening of customers during onboarding process against the list of high-risk countries.
* The system must have a Journal of AML check execution that shows in real-time all operations that fall under AML checks during the Onboarding process.
  + 1. **Requirements for Risk Profiling:**
* The system shall be able to configure AML risk factors to calculate final risk score of the customer (the system should be able to assign a high risk to a client based on a combination of two or more attributes).
* The system shall support customer AML risk classification.
* Any action related to the upgrade, downgrade or re-confirmation of client AML risk profile shall be traceable=> The solution must automate periodic KYC review workflow based on client segment and his risk scoring of the customer (for example, each year for High-risk customers, 3 years for medium risk customer, etc.)
* The system shall support to flag the customer for review during ongoing monitoring process.
* The solution must trigger KYC review workflow based on manual or automated triggering events (Submission of STR, hit with adverse media, combination of such attributes as turnover above the threshold and non-resident status etc.).

**Module 2: Transaction Monitoring & Anti-Money Laundering:**

1. **AML Rule Engine:**

* Implementation of advanced detection methodologies to analyze transaction and KYC pattern/behaviors.

1. **Alerts Management:**

* Alert generation based on predefined rules.
* Assignment of alerts (single/bulk) to appropriate personnel.
* Investigation workflow, evidence attachment, and closure process.

1. **Scenarios Monitoring:**

* General Scenarios (e.g., KYC, Transaction Limit monitoring, Threshold transactions, Quick Fund Transfer, Payment card and P2P transactions, Digital transactions, Circulation, Structuring/Smurfing, Business relevance).
* Special Scenarios: Capability to add and customize 20+ scenarios.

1. **User Maintenance and Security:**

* Multi-level Role Management.
* Integration and mapping with the Core Banking System, Pay logic, DFA, Mobile Banking/Internet Banking and any 3rd party systems.

1. **Alert Generation Setup:**

* Configuration of alert generation rules.
* Distribution and sending of alerts through emails and in Compliance/AML solution.

1. **Requirements for Clients’ ongoing monitoring**

* The system shall be able to review and re-screen customers in case of list updates and in case of matches escalate to compliance for further decision-making.
* Configuration and update of KYC forms and risk profiling of customers, and to allow the customization of KYC forms per subsidiary.
* Ability to Flag customers for EDD.
* The system must allow ad-hoc or scheduled scans for a certain category of customers, relations, against one or more lists chosen by the user.
* The system must ensure multi-criteria screening, option to integrate multiple scenarios without conflicting with each other to reduce false positives.
* The system should be able to create and maintain an Internal blacklists of clients: 1) for monitoring purposes, which must be able to upload all transactions of persons on this list for the previous day to the daily report; 2) Internal blacklist of clients that FINCA considers as non-acceptable and in case of matches the system should escalate to compliance for further decision-making.

1. **Requirements** **for Ongoing Monitoring of Transactions (Local and International):**

* The system shall be able to perform real-time screening of transactions against specific rules/scenarios (cash deposit, cash withdrawal, money transfers including SWIFT, Fast Money transfers, P2P card transfers, local transactions etc): Sender, Receiver, Sender Bank, Receiver Bank, correspondent bank, purpose of payment etc.
* The system shall be able to perform real-time screening of transactions against watch-lists, including the list of high-risk countries and Internal blacklist of clients (cash deposit, cash withdrawal, money transfers including SWIFT, Fast Money transfers, P2P card transfers, local transactions etc): Sender, Receiver, Sender Bank, Receiver Bank, correspondent bank etc., at the same time all transactions on which matches are detected must be reflected and recorded in the Journal of AML check execution in real time.
* The system shall be able to screen local/international transactions in relation to the level of AML risk associated with the customer.
* The system shall be able to set the thresholds for transactions’ real-time screening, as well as post-factum (with the possibility of setting different product-specific thresholds).
* The system shall support multi-criteria screening (pre-defines scenarios)
* The system shall be able according to pre-defined scenarios to escalate high risk transactions for review and approval of compliance officer.
* The system must allow to put in hold transactions matching any list or rule in order to be blocked or released by authorized teams .
  + Transaction approval/postpone/rejection decisions shall be traceable and shall have an option to document justification.
  + The system shall be able to perform real-time screening of transactions against specific "Keyword List" with the possibility of transaction blocking (cash deposit, cash withdrawal, money transfers including SWIFT, Fast Money transfers, P2P card transfers, local transactions etc): Sender, Receiver, Sender Bank, Receiver Bank, correspondent bank, purpose of payment etc. (depending on the choice of setting).
  + The system shall be able to perform real-time screening of transactions against watch-lists, including the list of high-risk countries and Internal blacklists of clients during the launch of the automatically configured Jobs in the CBS, and during crediting funds to customers' accounts by a one file/list (e.g. when depositing wages to the Bank's clients by a single file/list within the framework of salary, pensions projects in the Bank, or setting up scheduled loan repayment, which on certain dates the ABS automatically deducts money from the client's accounts and sends it to loan repayment).
  + The system should be able to check card transactions against all watch-lists, after uploading card transactions from the Processing Centre to CBS and block transactions in case of a match.
  + Receive alerts when matches with defined scenarios are detected.

1. **Case management:**

Ability to monitor and flag clients’ transactional suspicious and unusual behavior, patterns, transaction history, third-party, prior cases etc.

1. **Requirements for Audit trail:**
   * The system shall be able to keep the history and traceability of the various actions carried out by users and System.
   * The system shall have ability to export audit report.
   * The system shall have possibility to choose the fields to export, choose the audit period (start date and end date).
   * Ensure traceability to any version of a client KYC information (data, documents, workflow etc).
2. **Other requirements**:
   * The system shall be able to monitor digital transactions.
   * The system shall be able to detect log-in locations into the mobile applications/internet banking from different locations.
   * Support visualization of relationships between transactions, customers, accounts, and locations.
   * Manage alerts through integrated alerts and case management with predefined workflows.
   * Reduce false positives.
   * The system shall be able to import client information from CBS to the AML system supporting for decision-making and be able to export to CBS decision-made by compliance function.

**IV. Reporting:**

**Requirements for** **Reporting**:

* + Ability to automate Filing and reporting of STRs/CTRs to State Financial Intelligence Service.
  + The system shall have the audit trail, logs for reporting and acceptance of reports by State Financial Intelligence Service.
  + The system shall support integration of customizable dashboard.
  + The system shall have decision-making reports on the processing of alerts.
  + The system shall support visualization of reporting.
  + There should be a single Transaction Control Journal/Report in the system, which should contain all transactions for the previous day that fall under the automated AML controls in the Ongoing Monitoring of Transactions process (with the possibility of filtering).

**Comprehensive Reporting:**

Generation and uploading of comprehensive reports on compliance status, alerts, and investigations.

**Audit Trail:**

Maintain a detailed audit trail for all user activities within the system.

**V. Implementation and Timeline:**

Detailed implementation plan with milestones, and user training.

## 3.2 Technical requirements

**Reporting Requirements**

* Built-In or Integrated Reporting Module / Platform, offering a set of preliminary designed reports and business intelligence (BI) features that can accurately monitor and measure customer service factors.
* Ability to develop additional and modified reports and dashboards (without Vendor Support services) using the reporting platform offered by the system.
* Support for Ad-hoc reports and Dashboards (through embedded or integrated tool) - allowing system users to easily create customized reports and dashboards without scripting.
* Availability of Filtered Views, enabling access to system data through SQL.

**Documentation and training requirements**

Availability of up-to-date documentation for the acquired system, including (but not limited to) the following:

* Functionality description and parameterization guide.
* Software architecture.
* Deployment architecture and instructions.
* Integration framework.
* Data dictionary and Entity Relationship Diagram.
* Installation instructions.
* Troubleshooting Guide.
* Error Guide.
* User Manual.

**Architecture:**

* Web-based architecture, compatible with major web browsers (such as: Microsoft Edge, Google Chrome). Browser agnostic solutions are preferable.
* Mobile Optimized or Responsive Web User Interface.
* Layered (Three / N-Tier) architecture. Software should be engineered to have the processing, data management and presentation functions (layers/tiers) physically and logically separated. These different functions (layers/tiers) will be hosted on several machines or clusters, ensuring that services are provided without resources being shared and, as such, these services are delivered at top capacity.
* Modular architecture –system functions must be separated into independent pieces or building blocks, each containing all the parts needed to execute a single aspect of the functionality. Together, the modules make up the executable system.
* The system should support multiple integration technologies, including the common API standards and protocols, such as: SOAP, XML-RPC, JSON-RPC, REST.
* Integration features of the system should support:
  + Synchronous and Asynchronous nature of API function.
  + Event-driven and Data-driven integrations.
* Support of batch data upload through (CSV or other flat format) - single or package file modes.
* Capability for publishing the Custom APIs (without vendor support services).
* Versions of all environment software components (such as: OS, DBMS, Middleware, Runtime, etc.) of system must be on active support by manufacturer.
* The technology should have an architecture that enables the deployment of disaster recovery environments without restrictions of RTO and RPO.
* The system should be certified for deployment within a Highly Virtualized environment.
* "Cloud ready" system – The system should be compatible with cloud-hosted environments.

**Parametrization / Workflow Capability:**

* System functionality should support Process Management / Workflow capability – allowing:
  + Graphical User Interface to support creation of business processes specific to service, product or transaction (preferably - drag & drop based).
  + Ability to configure automated and user-driven activities for each step of the business process.
  + Definition of access rights for user groups / roles - for specific stage of the workflow.
  + Workflows triggered based on specific conditions (in addition to manual initiation by the users).
* At each stage of a process configured in the system, functionality is expected to:
  + Allow to inquire data from external (integrated) sources;
  + Allow to hand over data and/or initiate events and transactions in integrated systems and interfaces (through supported API framework);
  + Allow mathematical and logical operations over the captures and inquired data and process next step based on result.
* Produce an audit trail for operations processed through the system workflow.

**Scalability:**

The system should be able to handle a growing transaction base and increased usage without significant performance degradation.

**Security:**

* The Connection between User Interface and System Service should be secured via an up-to-date protocol (SSL encrypted through the latest available and non-compromised algorithms).
* The System should implement secure authentication mechanisms to verify the identity of users and ensure proper authorization for accessing sensitive features and data.
* Each user must have a unique user ID and authentication credentials. All credentials should be managed from a centralized console, either through Active Directory or specific to the System.
* If the System cannot be integrated with FINCA corporate Active Directory:  
  The System should allow configuration of requirements for strong user password - such as: length, age and complexity criteria.
* If the System cannot be integrated with FINCA corporate Active Directory: The System should support Multi-Factor Authentication for remotely connected users.
* The System should support the definition of user roles and configuration of permissions for data access, transaction processing and authorization (for each role). The System should support segregation of duties including access controls to prevent users from viewing data without explicit authorization (e.g., each user can only view data within their own unit and consistent with their job function).
* The System’s features should allow restriction of unauthorized data deletion.
* Implementation of security controls against OWASP TOP 10 attacks (URL, XSS, SQL, API injections etc).
* Security scan (SAST/DAST) and code vulnerability reporting must be provided prior to project delivery.
* Remediation of vulnerabilities identified by the Bank within the framework of a technical support agreement or contract.
* Session management in accordance with best practices (secure algorithms and random generation of session identifiers, termination of session upon log-off, session inactivity timeout, generation of new session identifier when a user re-authenticates, periodic termitation of sessions).

**Data privacy:**

The System should comply with data protection regulations of Kyrgyz Republic and ensure the privacy and confidentiality of users' personal and financial information.

**Secure storage:**

User data stored within the System or on the server should be protected using strong encryption and access control measures.

**Error handling and recovery:**

The System should handle errors gracefully and provide appropriate error messages to users, with mechanisms in place for data recovery in case of failures.

**Usability and user experience:**

The System should have a clear and intuitive interface, with easy navigation and well-organized menus and controls.

**Consistent design:**

The System should maintain consistent design elements throughout the user interface to create a cohesive and recognizable user experience.

**Accessibility:**

The System should comply with accessibility guidelines and provide features to accommodate users with disabilities, such as support for screen readers and adjustable font sizes.

**Multilingual support:**

The System should support multiple languages (Russian, English) to cater to a diverse user base and provide a localized experience for different regions.

**Performance monitoring and analytics:**

* Tracking and monitoring: The System should have built-in tools for monitoring performance metrics, such as response times, error rates, and resource usage, to identify and address any performance bottlenecks.

**Support and maintance:**

* The vendor should provide reliable technical support (available in different time zones) and assistance to address any issues or queries related to the app's functionality or usage.
* Availability of Service Level Agreement for technical support by manufacturer with clear defined classification of incidents and responses accordingly. Support and maintenance of all components of System by manufacturer should be included:  
  - obtain of new version of System;  
  - functional development or customization of System by request;  
  - fixing known vulnerabilities and patching of all components of System;  
  - adaptation of System to new versions of components (such as: OS, DBMS, Middleware, Runtime, etc.).
* Ability to share source code or other options to mitigate third party risk to acceptable level.
* Regular updates and maintenance: The System should receive regular updates and maintenance to address bugs, security vulnerabilities, and compatibility issues, ensuring its long-term reliability and performance.

# 4. Response terms and conditions

The following response terms and conditions have been defined to ensure the most fair and efficient selection process as possible:

* The contents of this RFP are deemed confidential and are provided to you for purposes of responding to this RFP. This information may not be disclosed to others without the express written consent of an authorized representative of FINCA Kyrgyzstan.
* Information submitted in response to this RFP will become the property of FINCA; FINCA will not pay for any information herein requested, and FINCA shall not be liable for any costs incurred by any supplier.
* FINCA has no obligation to disclose bidders’ identities to other bidders.
* Any information contained in the Response that is proprietary or confidential must be clearly designated. FINCA will reasonably maintain the confidentiality of Vendor’s Confidential information if directly marked "Confidential Information"
* Prime contractor or other involved parties (if different than the software publishing company) should be identified with appropriate contact names and phone numbers.
* FINCA will not reimburse any Vendor or respondent for any costs associated with preparing a response to this RFP.
* Attempts to communicate with the company outside of the process outlined in this RFP could result in your company’s removal from the vendor selection process.
* Cooperating with and adhering to this time frame and process will be a factor in considering your product as a potential solution.

# 5. Contents of proposal

Please submit your proposal utilizing the format detailed below within this section.

All responses are to be incorporated through pre-determined response templates annexed to this document.

Please do not delete rows/columns within the response template in your proposal submission.

Please be sure to include in your response sufficiently detailed explanations of the current status of requested business and technical requirements. **Responses that lack details explaining the functionality of your System will be viewed unfavorably.**

If you feel an answer requires detailed information (reference to an attachment), please indicate the reference to the additional information in respective section of the response template and provide additional information as an attachment to the template.

## 5.1 Appendix A: Vendor’s response template

The template consists of five worksheets dedicated to company, product and partner companies.

Submit your responses in cells next to the question. Please, add columns for additional products and companies as necessary.

* **Company profile** – complete sections related to company profile and major customers. Provide information about your major customers (banks and financial Institutions). In addition, please, indicate your customers located in the countries of the above subsidiaries.
* **Product Information** – Provide information related to the proposed system capabilities against the requirements stated under Paragraph 3 of this document. Including: current proposed version, functional capabilities, new and enhanced features, and your product’s road map detailing future enhancements of your product, etc.
* **Licensing and Support** – provide information about licensing and support terms for all products referred in “Product Information” worksheet.
* **Implementation and consulting** – provide information about terms of consulting services for all products referred in “Product Information” worksheet.
* **Partner companies** – list your partner companies, providing the listed types of services to your products.

## 5.2 Appendix B: Business Requirements

The appendix document contains information regarding the detailed business requirements that FINCA requires from a candidate for the development/delivery of the Compliance and Anti-Money Laundering solution .

Submit your responses under the following columns of Functionality Requirements and Technical Requirements worksheets:

| **Column** | **Instruction** |
| --- | --- |
| Support Status | Indicate relevant support status for each requirement:  • Fully Supported  • Partially Supported  • Not supported; Can be customized  • Not supported; Cannot be customized |
| Functionality Description | Describe system functionality against the required features. |
| Additional Comments | Additional Comments (Optional) |

**5.3 Appendix C: Total cost of ownership template**

### 5.3.1. License and support

Please provide information about the cost of your proposed license and support fees associated with System and software required for its deployment – database, operating System, middleware and other third-party applications.

### 5.3.2 Implementation

Please provide a detailed breakdown of the costs anticipated during system implementation phase.

* **Consulting Services –** indicate number of consultants engaged in implementation project, providing estimated terms of engagement and associated rates; Estimate consultancy fees related to each phase of overall implementation activity.
* **Travel, accommodation, incidentals –** provide estimated cost associated with onsite presence of system consulting team (travel, accommodation, incidentals).
* **System customization costs** – costs related to customization and localization changes essential for delivery of required functionality features (Appendix B: Business Requirements).
* **Implementation of third-party Systems** – costs associated with implementation of any third-party System required for deployment of system (if applicable).
* **Additional costs –** Please describe any other commercial terms FINCA should be aware of.

## 5.4 Additional documentation

### 5.4.1 Team resumes

Please provide resumes and professional certifications of the proposed team members. Summarize the experience of the engagement team with respect to coordination and responsibilities inherent in completing an integration of this scope and complexity.

### 5.4.2 Project organizational chart

Describe the engagement team organization, how the engagement will be coordinated, and how this engagement management approach will contribute to the efficiency and cost effectiveness of the project. Be sure to provide details on any offshore resources that will be used.

### 5.4.3 Subcontracting

Identify your firm’s approach to staffing portions of this engagement with subcontracted labor.

### 5.4.4 References

Provide a list of three to five references that may be contacted for each member of the engagement team to allow for an independent view of their approach to client service.

Describe what you believe are the key areas the selected engagement team will assist us in the successful implementation of the system. Also, provide examples of what your engagement team members and your firm have provided to clients that display your commitment to quality and client satisfaction.

# 6. Selection criteria

## 6.1 Evaluation of responses

The vendor and software product selection decision will be based upon the high-level criteria detailed below. We reserve the right to add additional criteria and to determine weighting of criteria for determining the final solution software and vendor. No vendor submitting information based upon this RFP has a proprietary interest or automatic rights to selection, regardless of past contractual/project history with FINCA.

| **Scoring criteria** |
| --- |
| **Vendor experience and qualifications** – demonstrated experience and qualifications to assess the ability to deploy successfully in an environment similar to FINCA’s (e.g., industry experience, implementation methodology, ability to manage implementation risks, and mitigation strategies). |
| **Functionality features** – ability of system to meet FINCA’s stated business requirements and integrate into or enhance FINCA’s business processes. Additionally, fit with our existing architecture and application landscape will be a key consideration. |
| **Technology platform** – upgradable and scalable technology platform that enables stable performance and easy integration. |
| **Information security compliance -** Information security management system in place in the vendor’s company ensuring information security in development and support services, as well as compliance with regulations in the area of personal data protection and information security. |
| **Ease of implementation, use and support** – for the delivery of the Compliance and Anti-Money Laundering solution’s perceived adaptability amongst the end-user community within FINCA’s global organization (e.g., intuitive user interface, ease of deployment, ease of ongoing maintenance, local support, specifically in regional time zones and in FINCA’s official languages). |
| **Total cost of ownership** –Total cost of ownership (e.g., initial and ongoing software license and maintenance costs, infrastructure acquisition costs, System customization costs, Systems integration labor costs, and organizational training costs). |

FINCA will analyze the responses from vendors using a scoring methodology. Each respondent will be evaluated based on the completeness of the requirement responses.

## 6.2 Vendor demonstrations and score validation

Selected vendors will be invited to demonstrate the capabilities of their product to decision stakeholders in a structured setting that leverages FINCA-developed demonstration scenarios.

FINCA will evaluate vendors’ demonstrations to grade on the quality of product, industry experience, ability to partner, ease of adoption, and demonstrated knowledge of FINCA’s business (i.e., adherence to provided demonstration scripts). FINCA reserves the right to add or modify the selection criteria at any time.

## 6.3 Reference checks

FINCA requests the option to contact your existing customers to discuss system capabilities, product satisfaction and implementation experiences.

FINCA reserves the right to perform necessary background check and references and qualifications checks as deemed necessary.

## 6.4 Vendor selection

The selected vendor will be identified solely by the judgment and discretion of FINCA. The vendors will be evaluated based on how fully each demonstration and proposal meets the requirements of this RFP.

# 7. Communication and Q&A protocol

We acknowledge that vendors might have questions regarding the RFP, as well as the requirements outlined herein. To assist in helping you to become well equipped to respond effectively to our needs, we are offering to make delivery of the Compliance and Anti-Money Laundering solution PMO available in the following ways:

## 7.1 Written inquiries

Until July 25, 2024, all candidate vendors may be able to submit written inquiries, which will be answered within 5 working days from the date of submission.

## 7.2 Vendor demonstrations

During the period from September 4, 2024 to September 19, 2024, a vendor demonstration event will be held where selected candidates will be provided with the opportunity to showcase their products and service capabilities in the context of FINCA’s business requirements. The place will be informed to the selected candidates.

The vendor demonstration requests will be delivered to selected vendors only. The request will be delivered along with the demonstration agenda, which will provide the “playbook” from which FINCA will ask vendors to conduct the demonstration.

Please note that adherence to the demonstration agenda will be extremely important as it will allow the business to assess the delivery of the Compliance and Anti-Money Laundering solution in the context of the business, but also will demonstrate the vendor’s ability to partner with FINCA and listen to its needs.

# 8. Next Steps

As noted above, FINCA is beginning the process of selecting their system. Completed proposals must be submitted based on the date specified in the timetable provided under paragraph **2.1 RFP process schedule.**

FINCA reserves a right to modify above mentioned planned activities as well as proposed timeframes at any time.

The RFP responses are due by August 12, 2024

It is preferred that responses are submitted via email with completed appendices attached (A - Vendor Response Template; B - Business Requirements; C - Total cost of ownership).

Questions regarding the RFP document should be directed to:

|  |  |
| --- | --- |
| Email: | [zhyldyz.sultanbekova@finca.kg](mailto:zhyldyz.sultanbekova@finca.kg) |
| Address: | Kyrgyzstan, Bishkek, 93/2 Chopokova Street |
| Website: | https://fincabank.kg/ |