Request for Proposal

Purchase of Operational Risk Management Tool / Solution

Dear Sir / Madame,

Union Bank invites you to participate in the tender process for "Purchase of Operational Risk Management Tool”.

The purpose of this Request for Proposal is to accept; evaluate and select the best Proposal that meets the Bank's requirements for this process, according to the requirements listed in this Request for Proposal.

The proposals will be evaluated in accordance with the selection criteria below that will determine the winning bid:

- Technical evaluation of the proposed solutions / Tools, offered by the company for the requested services.
- Commercial evaluation based on the best and final price offered.

Thank you in advance for your reply and best regards,

Date issued 9 May 2024

TABLE OF CONTENTS

1. **Introduction** 3

2. **Functional Requirements - Summary** ……………………………………………………… .3

3. **Functional Requirements - Detailed** ……………………………………………………..…...3

4 **Required functionalities ………………………………………………………………..….. 4**

5. **Project Organization & Governance** 9

6. **Request for Proposal Timeline** 10

7. **Annex 1: List of Proposal Documentation ………………………………………….……..**11

1. Introduction

Union Bank (hereinafter “the Bank”, or “UB”) is a financial institution registered as a Commercial Bank on 9 January 2006. For further information regarding the Bank’s activities, size, and financial situation, please visit our website: www.unionbank.al.

2. Functional Requirements - Summary

To properly identify, assess, mitigate, and monitor the operational risk, it is required to have a system/tool for the management of the operational risk.

The system will have 7 main functions.

1. Operational Risk Event Reporting
2. RCSA (Risk and Control Self-Assessment)
3. KRI Report Administration
4. Risk Monitoring
5. Provisioning
6. Cost of Risk
7. User administration

3. Functional Requirements - Detailed

3.1 Existing Functionality (describe the existing functionality of the service/system/application)

3.2 Operational Risk Event Reporting

The reporting unit prepare the risk event reporting form and submit it via email to the Risk Department.

The Risk Department Officer register the event in excel sheet which serve as database for administration of risk event.

From the excel file that serve as the risk event administration the Risk Department Officer prepare different reports concerning the risk category, the unit involved, the financial impact, refunded amount. Also perform follow up for the action to be taken from the reporting unit after the event occurrence.

The Risk Department Officer monitor different GL accounts to verify the financial impact of the event and the refunded amount.

3.3 RCSA (Risk and Control Self-Assessment)

The risk taxonomy used for the yearly Risk and Control Self-Assessment, populated with the data and information gathered during the interviews with operational risk correspondents from all the Bank’ units/departments, will be recorded in an excel file (including methodology used for the determination of risk severity – i.e. high/medium/low). Such information shall be further recorded in the Operational Risk Tool/Solution, for further processing and analysis.

3.4 KRI Report Administration

Bank units frequently report the KRI for indicators under their responsibility. Every KRI report is stored in share folders of the Risk Department and are further elaborated based on their status.

3.5 Risk Monitoring

The Risk Department Officer monitor different GL accounts to verify the financial impact of the event and the refunded amount.

3.6 Provisioning

The Risk Department Officer monitor in monthly bases the loan provisioning process. The monitoring consists in verifying the amount register in GL account maintained for the accounting of loan provisioning.

3.7 Cost of Risk

The Risk Department Officer calculate the cost of risk for the risk event reported that have a financial impact. The calculation is based on the gross financial loss reported and the refund (if any) done for the event.

4 Required functionalities (describe the exact changes that you request on the service / system / application)

4.1 Operational Risk Management Tool

To properly identify, assess, mitigate, and monitor the operational risk it is required to have a system for the management of the operational risk.
The system menu will be defined from functions description. There will be 6 main functions in the menu.

Function description	Attributes
Operational Risk Event Reporting	The user will be able to submit the report through manual data input. The fields that will be inputted are predefined. The option of data upload through an excel file (form) shall be available also.
KRI Report Administration	The user will be able to submit the report through manual data input. The fields that will be inputted are predefined. The option of data upload through an excel file (form) shall be available also.
Risk Monitoring	Available report already processed from other bank system will be integrated in the new platform.
Provisioning	The platform will use the data collected from core banking system (records by Finance/Accounting Unit in respective GLs).

Cost of Risk	The platform will use the data provided through operational risk event reporting and from data collected from core banking system regarding the expenses incurred
User administration	A limit number of users will have access to the platform. The Risk Department users will have the attribute of system administrator. 4 Eyes principle shall exist for every data input / modification / cancelation - i.e. one user inputs the information in the Tool, another user (supervisor) authorizes the record.
Audit Logs	The tool shall offer also the possibility of verification of Logs (related to user activity), in order to be able to identify deleted data / records, modified data / records, etc.
Data / Reports for Risk Analysis	Beside of the reports already available/customized in the Tool, the extraction of other data / customizable reports shall be possible, for further risk analysis / statistics.

1. Operational risk event reporting

During the event occurrence the user that will have the rights to report the event will input the event in the platform after the successfully log in. There will be distinct forms for each event category. The form should contain the below fields.

Number	Event Category	Value type
1	Event Details	
	Event description	String
	Reporting Unit	List of Value
	Event Occurrence Date	Date
	Event discovery Date	Date
	Comments	String
	Recurrence number	List of Value
	Units involved	String
	Cases involved	String
	Comments	String
	Customer involved	String
	Comments	String
	Financial impact	List of Value
	Comments	String
	Refund	List of Value
	Comments	String
2	Financial impact details	
	Currency	List of Value

	Gross amount	Number
	Account Number	String
	Comment	String
	Refund amount	Number
	Net loss amount	Number
	Refund Type	List of Value
	Refund Date	Date
	Refund account details	String
3	Risk Category	
	Risk Category	List of Value
	Risk Subcategory	List of Value
	Detailed Classification	List of Value
	Code	Number
	Cause	List of Value
	Business Line	List of Value
	Credit/market related or Fraud	List of Value
4	Remarks	
	Detailed description of event	String
	Detailed description of actions taken after the event	String
	Proposals to prevent the occurrence in the future	String
	Event status	List of Value
5	Risk Department Evaluation	
	Gross loss amount	Number
	Total refunded amount	Number
	Net losses amount	Number
	Exchange Rate	Number
	Event Type	List of Value
	Event Classification	List of Value

After the input and save of the event reporting the platform will assign a unique number to the form. The reference number will be composed from the

- 6-character date of event. Format YYMMDD
- 3-character of the event category
- 3-character sequential number starting from 001

The reference will serve to identify the report allowing the user to search in the event view summary.
Once authorize from the users with the appropriate rights the event report will be definitive with no possibility to amend the event report.

The reported event can be cancelled from the Risk Department. Once authorized the cancelation the report will not be active anymore.

2. Risk and Control Self-Assessment

Information on the RCSA will be initially inputted in an excel file, where the defined risk taxonomy contains mainly the following information for every process analyzed (assessed):

- Activity
- Domain
- Process Name
- Sub-Process Name
- Process Description
- Process Scope
- Process periodicity
- Information on Controls performed (level 1, level 2, permanent control plan, level 2.2) – description of control performed, typology of control (detective/preventive), classification (review, system authorization, reconciliation, etc.), responsible person / function for performing the control, etc.
- Risk Identification (from a drop down menu – risks as per Basel definition).
- Worst Scenario Analysis
- Historical Losses identified for the process
- Losses in worst case scenario
- Financial Impact Assessment
- Non-Financial Impact Assessment
- Assessment of Risk Severity based on pre-defined risk criteria (impact, likelihood). Risks are assessed as Low, Medium, High
- Assessment of Control Environment (from a drop down list)
- Action Plans proposed at the end of the process assessment (form improvement of the process, control environment, etc.)
- Etc.

3. KRI Report Administration

The KRI Report should be submitted through upload operations.
The fields available for each category are.

Number	Unit/Department	Value type
1	Loan Admin	
	Percentage of processed applications with errors	Pct.
	Percentage of unregistered collaterals	Pct.
	Collateral with insurance expired	Pct.
	Loan workouts - Difference of market and recovery value of the collateral	Pct.
2	Accounting	
	Bank's debtors position accounts, accounting node A4 117 - Total duration	Number
3	Credit Risk Division	

	Number of corporate/ sme reviews overdue	Number
	Monthly average loans downgraded to SPM during the quarter	Pct.
	Monthly average loans downgraded to SBS during the quarter	Pct.
	Collateral - Percentage of cases collateral signed without on-site inspection	Pct.
	Concentration of collateral assessments	Pct.
	Collateral - Percentage of Housing loans with insufficient collateral ratio	Pct.
4	HR	
	Number of staff non-compliant with Holiday regulations	Number
	Staff turnover percentage	Pct.
	Number of training days per employees (applicable to operational staff only)	Number
	Number of employees with sick days above the threshold	Number
5	IT	
	FCC outages	Number
	LAN & WAN outages	Pct.
	Attacks on bank's IT system	Number
	Daily EoD process (start time)	Number
	Daily EoD process (duration)	Number
	FCC - UB Banking Web interface outages	Number
	FCC - Mobile Banking interface outages	Number
6	Payments	
	Number of back-valued deals initiated in Treasury	Number
	Unreconciled transactions between Treasury and Back Office	Number
	Claims from clients, customers, generated on ATM withdrawals	Pct.
	ATM shortages - Number	Number
	Number of fraudulent transactions in cards activity	Pct.
	Number of fraudulent transactions in cards activity	Pct.
	Total number of incorrect outgoing payments	Number
7	Operations	
	Errors per employee rate	Number
	Tellers' differences (value)	Number
	Tellers' differences (number)	Number
8	Security	
	Problems related to electronic security systems	Number

	Number of cases identified of non-compliance with security procedures	Number
	Number of critical security incidents	Number
9	Internal Audit	
	Overdue Internal Audit issues	Pct.
10	Compliance	
	Regulator's/ Authorities' issues not implemented	Pct.
11	All Divisions	
	Frauds - Number detected	Number
12	Retail	
	Complaints from clients, intermediaries (except ATM claims)	Number

The KRI report values can be amended from Risk Department.

4. Risk Monitoring

The monitoring reports will be produced from bank reporting system. For each category there will be a limited number of reports. The available reports are generated in Excel or Pdf. The Risk Department users can generate the report.

5. Provisioning

The function provisioning will use the data collected from core banking system.

6. Cost of Risk

The platform will use the data provided through operational risk event reporting and from data collected from core banking system regarding the expenses incurred.

7. User administration

The number of users that will have access to the platform will be around 20 to 50. The users’ rights will be administrated from the Risk Department. The user will have access to the function and submenu specified as per their user rights.

5. Project Organization & Governance

Project Management methodology will be defined accordingly, based on the proposal submitted by you in the technical proposal document.

Bank will contribute to project quality assurance during implementation, data migration strategy & approach as well as User Acceptance criteria tests.

6. Request for Proposal Timeline

Date	**Event**
9 May 2024	RFP Issued
14 May 2024	Deadline for submitting questions, clarifications
16 May 2024	Deadline for the Bank to submit the answers
22 May 2024	Deadline for bidders to submit proposals
14 June 2024	Deadline for the Bank to Notify selections
21 June 2024	Contract sign off

Proposals must be received on or before the deadline and submitted by email to **procurement@unionbank.al**

The proposal format must contain the list of documentation included in Annex 1 attached to this RFP.

The offer must remain valid for a period of at least 180 days from the date of the submission.

ANNEX 1: List of Proposal Documentation:

Your proposal should include, but not be limited to, the following elements:

1) Solution Overview: A detailed description of proposed Tool /Solution, emphasizing how it specifically accomplishes the functions in scope of the bank’s requirements.
2) Administrative information / vendor profile (mailing address, phone number of designated point of contact). Key profiles of the company and detailed CV-s of the resources that will be engaged the bank's project.
3) Project management approach (Including key project risk monitoring Procedure),
4) Implementation and Support: A clear implementation type (on-prem/cloud/SaaS, etc.), plan, timeline, and details on the nature of ongoing support and maintenance services.
5) Hardware, Operating System, and database (if needed) requirements,
6) Professional Training. A detailed outline of the training program, including curriculum, format, duration, trainer qualifications, and post-training support.
7) Proof of Concept**:** The possibility of conducting a POC, for a trial period, to understand if the tool may have any impact on specific systems or applications.
8) Technical Specifications: System requirements, compatibility with existing infrastructure, and any hardware or software prerequisites.
9) Client References: List of respective solution implementations performed in the last 5 years, specifying the bank/institution, the core platform integrated into and respective references. References of previous experiences of implementation of your solution to be provided.
10) Draft Contract template: A draft contract template for the requested Tool / Solution must be provided together with the other required documentations.

11) Pricing Structure: Detailed pricing information, including any setup fees, subscription models, maintenance costs, and additional charges for training services. Commercial Proposal must include:

- Total commercial proposal for the solution/s proposed
- Breakdown of applicable fees into phases of the project
- Conditions and deliverables for payments

Currency shall be in EUR, to be specified VAT and / or any other applicable tax included or not.

Subcontracting will NOT be allowed during the realization of the contract, except with prior Bank approval. In case verified, it will lead to immediate interruption of the Contract.

The Bank reserves the right to continue the process with the Bidder that will better match the bank’s expectations in terms of both technical and financial parameters.

To ensure same level of information for all participants, whatever answer, or additional clarification that the Bank will give to one of the interested companies, will be shared with the rest of the participants in this process.

As a result of this request, a contract will be concluded with the selected Supplier.

Partial bidding is allowed in this RFP and such offers will be accepted.

Subcontracting will NOT be allowed during the realization of the contract, except when approved prior by the Bank. In case verified, it will lead to immediate interruption of the Contract.

To ensure same level of information for all participants, whatever answer or additional clarification that the Bank will give to one of the interested companies, will be shared with the rest of the participants in this process.

The form of communication for any question regarding the scope of this Request for Proposal will be done only through the e-mail address: procurement@unionbank.al

The Documentation requested must be submitted in a **sealed envelope** by **May 22nd, 2024**, to the following address:

Departamenti i Administrates
Union Bank SHA
Bulevardi Zogu I, Sheshi Ferenc Nopçka, Nd. 5, H. 3, Njësia Bashkiake Nr. 9, Kodi Postar 1016, Tiranë, Shqipëri

With reference: ***"Purchase of Operational Risk Management Tool / Solution"***

Or in electronic version by email to the address: procurement@unionbank.al