

The New Development Bank

Request for Proposal

(This is not a Purchase Order)

1. Introduction

The New Development Bank (NDB) is issuing a Request for Proposal (RFP) to invite qualified suppliers to provide proposals to NDB's RFP S-IT-2024-01455 Integrated Risk Management Platform project. Please refer to the following information and attachment for detailed requirements.

Those interested and qualified companies please register into NDB's e-procurement system to be **NDB's registered suppliers** and participate in the bidding process (**please be noted the contact information provided in registration especially email address must be correct as all communications regarding the bid including RFP distribution and award notice will be sent through it**). NDB will choose the most suitable one(s) from the shortlisted suppliers. NDB at its sole discretion reserves the right to reject all proposals in accordance with its internal policy and guidelines.

2. RFP Schedule

Please be noted the following activities could take place in the RFP process. NDB will inform the specific arrangements in advance and the suppliers are requested to respond timely.

Activity	Date
Distribution of RFP	March 12, 2024
Deadline for Questions	March 20, 2024
Proposal Response Due	April 3, 2024
Presentation and Demonstration	TBD
Signing Contract	TBD
Project Kick Off	TBD

**The RFP Schedule is for reference only and NDB has its sole discretion to adjust as per the project's needs.*

3. Instruction to bidders

3.1 Contact Information

Please use the following contact information for all correspondence with NDB concerning this RFP.

Name: Junfeng (Jimmy), Wang

Address: 26th floor, NDB Headquarters, 1600 Guozhan Road, Pudong, Shanghai, China

中国上海浦东新区国展路 1600 号，新开发银行总部大楼 26 层

Email: wang.junfeng@ndb.int

3.2 Submission of Proposals (Introduction to use of NDB's e-procurement system)

Proposals shall be prepared in English. Electronic version is obligatory and shall be sent online in NDB's e-procurement system.

For submission of proposal, the qualified suppliers should register to NDB's e-procurement system to be **NDB registered suppliers** (subject to NDB's internal approval) in advance. All registration information shall be in English except uploads of scanned or copied documents originally produced in other languages. Then registered suppliers need to **ENROLL** in the procurement notice (for open competitive bidding) or **ACCEPT** the invitation (for limited competitive bidding) before submitting proposal online according to the timeline: <https://www.ndb.int/procurement-opportunities/corporate-procurement/>

The mentioning of deadline, due time, closing date, etc. herein means Beijing time; and NDB's business time is from 9:00AM to 5:15PM in working days.

3.3 Questions

Please submit questions in writing by e-mail. Suppliers should refer to the specific RFP paragraph number and page and should quote the questioned passage. NDB will be prompt in responding to questions. All questions will be responded to as a group and sent to all suppliers. NDB will not provide feedback to questions raised beyond deadline.

3.4 Ownership of Materials

All materials submitted in response to this RFP become the property of NDB. Proposals and supporting materials will not be returned to suppliers.

3.5 Proposal Costs

NDB is not responsible for any costs incurred by the supplier in the preparation of the proposal or the site visit.

3.6 Proposal Format (if applicable)

NDB recommends that the proposal should contain **three** parts as follows. **The supplier may choose another proposal format as long as it suits the purpose.**

Volume 1 – Information on the suppliers. The supplier is required to provide the basic information in the attached table (attachment 2). Please fill out the table as complete as possible, where it applies. More information is more helpful for evaluating.

Volume 2 – Main Proposal

Section 1	Executive Summary
Section 2	Functional Section
Section 3	Technical Section
Section 4	Project Management Section
Section 5	Support Section

Volume 3 – Price Proposal – Should be separate but integral part of the proposal. The currency is **USD**; if quoting in other currencies, the exchange rate should be clearly defined. **The price shall be inclusive of applicable taxes (if not, please specify)**; and other charges shall also be clearly defined.

3.7 Validity Period

The proposal including pricing quotation shall be valid at least for 120 days.

3.8 RFP Amendments

New Development Bank reserves the right to amend this RFP any time prior to the closing date. Amendments will be issued only to suppliers who are going to complete a proposal.

3.9 Sub-contractor

NDB expects to negotiate and sign contract with one winning supplier. NDB will accept only complete solutions from a primary supplier and will not accept any incomplete proposals that are only cover part of the RFP. The prime supplier will be responsible for the management of all subcontractors. NDB will not accept any invoices from subcontractors or become part of any negotiations between a prime supplier and a subcontractor. If there is any sub-contractor involved or engaged by the supplier, it shall be clearly stated in the proposal.

3.10 Award Notification

NDB could negotiate with all shortlisted suppliers before deciding the winning supplier. And NDB reserves the right to negotiate further with the winning supplier before and in the contracting process. The award notification is sent to the winner online in the e-procurement system. NDB is not obliged to notify the bid outcome to unsuccessful suppliers.

4. Evaluation Criteria

The proposals will be reviewed and evaluated by NDB's team in accordance with the related policy and guidelines, especially the six principles (Economy, Efficiency, Competition, Transparency, Value for Money, Fit for Purpose) contained in NDB's corporate procurement policy. NDB is interested in obtaining a complete solution to the requirements contained in this RFP. Proposals that meet the proposal instructions and requirements will be given a thorough and objective review. Proposals that are late, or do not comply with proposal instructions, or take exceptions to mandatory requirements will be eliminated without further consideration. The following are the key factors that would be taken into consideration for evaluating the proposals.

i. Technical Approach and Methodology or Software Solution

Primary consideration will be given to meet the mandatory requirements as listed in this RFP.

The following are the main factors in the evaluation.

1. Meeting the requirements as stated in this RFP;
2. Understanding of the work to be performed;
3. Technical approach and methodology to accomplish the work;
4. Completeness and competence in addressing the scope of work.

ii. Project Management

NDB also believes that effective project management is essential for a successful implementation. Suppliers will be evaluated on the completeness and responsiveness of their project management plans and the project team assigned.

As part of the project management plan, suppliers must demonstrate adequate experiences in developing and implementing the requested project. NDB's confidence in the suppliers' ability to meet deadlines and successfully manage similar projects will be a primary consideration.

Special consideration is given to suppliers who propose a detailed project plan with sufficient breakdown of tasks and steps to demonstrate a complete understanding of the project.

iii. Pricing

NDB will consider pricing as part of the evaluation criteria. **Lowest price is not essential to win**; however, large pricing differentials between suppliers will be carefully examined. Price will be used as a final indicator for determining the supplier finalists when all other criteria have been normalized.

iv. Presentation and Demonstration

The performances and results of Presentation and Demonstration will be evaluation factors.

v. Support and Maintenance

NDB believes the ability to perform timely support is also an important factor for the success of this project. Therefore, suppliers should provide adequate information to demonstrate their capabilities to fulfill this task.

5. Contract

The participants shall review the service agreement template provided by NDB in advance. The use of NDB's version of service agreement is preferable. NDB Template for Service Agreement and NDB General Terms and Conditions for Procurement Contracts can be found on the NDB's official website:

<https://www.ndb.int/procurement-opportunities/corporate-procurement/>

Please especially be aware that being an international institution, NDB enjoys privileges and immunities granted in the Articles of Agreement (Agreement on the New Development Bank) (<https://www.ndb.int/>) and disputes will be held by a reputable international arbitration center. Preferable forum is Shanghai International Arbitration Center ("SHIAC") or any alternative forum in a neutral jurisdiction.

Attachment 1:

Service Scope (Statement on Work)

Automate the Operational Risk (OR) tools and methodologies of the Bank on the Integrated Risk Management Platform

Requirements Specification

Executive Summary

Project Description

NDB's Risk Management Department (RMD) drives implementation of Operational Risk (OR) methodologies and tools across departments as per its internal policies and guidelines. The methodologies are currently implemented through spreadsheet-based templates and the Bank aims to automate the process across the first line of defense and RMD with use of enterprise wide-solution based on Integrated Risk Management (IRM). Technical criterion for the solution or systems mandates the platform to be ranked within the Top 10 of recognized industry assessments such as the Gartner list or an equivalent authoritative ranking among the leaders. This ensures that the selected platform aligns with industry standards and has a proven track record of excellence.

Glossary

Term	Definitions
OR	Operational Risk
RMD	Risk Management Department
IRM	Integrated Risk Management
RCSA	Risk and Control Self Assessments

Functions and Features

1. Functional Requirements

Functional requirements define the features the service solution or system must provide.

Requirement 1: Review and standardization of NDB information (detailed in methodologies) and workflows.

NDB information standardization:

- As per industry standards
- Ensuring readiness for system input and configuration

Requirement 2: OR methodologies' implementation

Following are the OR areas required to be configured in the system:

- *OR incidents* (Losses, near misses):
 - Data fields as per internal template
 - Workflow for reporting of incidents by any employee, establishment of action plans, approval by department head, analysis (and future monitoring) by Operational Risk/ Risk Management Department
 - Consolidated reporting and analysis.
- *Risk and Control Self Assessments (RCSA)*:
 - Configuration of RCSA methodology as per internal methodology and rules
 - Assessment schema of inherent risk, control environment and system computation for residual risk rating (based on internal rules)
 - Workflows/ assignments between the assessed department and risk department
 - Mapping of action plans for residually very high/ high risks
 - Migrating library of risks and controls by department (already available in spreadsheet).
- Key Risk Indicators (KRI):
 - Configuring KRIs for departments (already available in spreadsheets)
 - Inputs ability/ mapping to relevant departments
 - Monitoring mechanism of the indicators by OR as part of Risk Management Department (RMD); Threshold based escalations and reporting.
 - Availability of KRI libraries, thresholds for reference is an added advantage.
- Control testing:
 - Testing specifications of controls (owners, frequency, etc.)
 - Workflow and testing samples/ files management
 - Testing reports
- Mitigation action plans:
 - Mitigation action plans linked to incidents, RCSA, KRI or other areas applicable to departments, with mapping of responsibilities and fields including:
 - Periodic monitoring/ update requirements and escalations as applicable
 - Upload of historical action plans in system based on template/ data available.
- OR external incidents (*separate database*):
 - OR external incident inputs as per template

- Workflow to include creation by second line of defense with review, attestation of controls by first line of defense.

The implementation in system is to be carried out as per the internal assessment scales and methodologies as per the prevailing OR templates (available in spreadsheets). The libraries associated to Requirement 2 are expected to have linkage.

Configuration of the elements and taxonomies are to be carried out considering ability to accommodate the future methodologies that the system would need to cater to in Phase 2, including:

- Business Continuity Management (BCM):
 - Link to the RCSAs library
 - Business Impact Assessments (BIA)
 - Business Continuity Plans (BCPs)
 - BCPs Testing

Requirement 3: User and workflow alignment:

IRM configuration mapping based on OR (Operations Risk) system roles, aligning as per three lines of defense principles

The roles and controls need to be implemented as per the groups defined during the requirements gathering and through the hierarchy pattern as defined by the Bank (HR system, etc.).

High level system roles envisaged:

- OR input user (First line of defense)
- OR authorization user (Supervisor – First line of defense)
- RMD review 1 (Second line of defense)
- RMD review 2 (Second line of defense)
- IT administration: user access management.
- The solution or system should provide out of the box groups or flexibility to create and manage groups, roles and responsibilities in the IRM platform standards.

Requirement 4: System integration and data requirements

The methodologies are expected to be implemented in Service-Now Integrated Risk Management system.

Support for integration and capabilities including:

- Linking system to Active Directory for user reference
- Rule based notification's ability to users through email, leveraging mail server
- Ability to upload historical data through spreadsheets.

Pre-existing data would need to be uploaded to the system. The data is available as spreadsheets for:

- OR incidents (and external incidents)
- RCSAs
- KRIs
- Mitigation action plans.
- Control tests.

Requirement 5: Training

IRM (OR methodologies) training programs/ content for each applicable user group.

Requirement 6: Service, system, and solution minimum requirements for integrated risk management system

Service, system and solution minimum requirements for integrated risk management system perspective

- The systems or solutions should be a SaaS platform and should align to the Integrated risk management framework defined by industry best practice independent agencies such as Gartner
- The service and solution should have periodic SOC certification (SOC 2 Type II) completed and should be accessible for NDB to assess and verify as and when required
- The system or solution should have inbuilt periodic vulnerability assessment (VA*) and penetration testing (PT) mechanism or should be provided with the report periodically from the provider to be reviewed by the NDB
- The system and solution has to have minimum and maximum SLAs defined or in line with the below SLA

Priority	Response (max)	Workaround SLA	Resolution	Resolution Targets
Critical	30 minutes	2 hours	4 hours	90%
High*	2 hours	4 hours	12 hours	90%
Medium*	12 hours	8 hours	48 hours	90%
Low*	24 hours	24 hours	72 hours	90%

- *The expected support hours is 24*7*365 days and the expected incident or case follow up update has to be every 1/2/12/24 hours respectively as per the priority respectively.

- The solution or system should have inbuilt roles, rights and users management in addition to the functional requirements in with segregation of duties for developer, users, admin and maintenance roles.
- The solution and system should provide readily available integration to privilege access management solutions in the market
- The solution of systems should have inbuilt encryption mechanism with independence to be applied for each record, users, data set to the granular level
- The solution or system should provide the capabilities to follow incident, change and problem management in line with the industry standard ITSM practices and align to NDB ITSM practices.
- The solution or systems inbuilt libraries or Integration with the framework libraries (SOX, NIST, ISO etc.) for operational risks: internal or external or aligned as per standard frameworks/ bodies would be an added advantage
- The solution or system should be provided with completeness and transparency of effort and cost for example (Licenses/subscription/implementation per module and the timeline). Expected cost of the changes or future advancement or new modules implementation
- The solution and system should cover the modules which will be implemented, and provide the flexibility to extend to the ones omitted.
- The solution and system should have default available controls, attestation automation out of the box capabilities as per the benchmarked industry solutions and system
- Customization of the framework for the approved controls, attestation etc.
- Preferably, the workflow lifecycle automation and could be customizable and implementable by internal NDB team via project handover with no dependency from the vendor.
- Ability for Integration with ITSM and Monitoring system within NDB
- Integration with other modules such business systems log, SOC (SIEM) for the risk reporting an incident reporting.
- Integration/ APIs/ ability to obtain risk related information from Bank's prevailing systems
- Service providers should have at least 4 Banking industry experience for facilitating phase wise implementation of Integrated Risk Management
- Should be able to record and transition all configuration from the current (practice/data/systems) to new systems
- Post implementation support for the stabilization period for 1 year
- Training and Handover with proper documents and sign offs
- Preferrable, the solution provides mobile apps and available for mobile device or mobile access management platforms.
- System should provide full automation and customization capabilities
- Preferably, the system and solution provide the capabilities of following automated test mechanism
- The system and solution should provide inbuilt mechanism to have audit trail for all changes on the system
- The system and solution should have inbuilt mechanism for the logging of all event in the system
- The system and solution should have inbuilt mechanism for the rollback of all configuration or changes etc. in the system

- The system and solution should provide the capability to integrate with other relevant NDB systems/ existing platform i.e. ITSM, NDB integration Platform as a service (IPaaS), HR system, NDB SIEM platform etc.
- All implementations should guarantee that there is no impact upon any changes or upgrades on the SaaS platform
- The UI (user interface) implementation should be inline of the business requirements of the NDB.
- The implementation team need to support the platform for a period of 6 months from the date of production go live. Additional BAU (business as usual) support should be proposed from the vendor for evaluation.
- The implementation must adhere to Information Security guidelines of NDB and signed off by the NDB Information Security team after production go live
- The high availability of the system, RTO (recovery time objective) and RPO (recovery point objective) of the system should be agreed and approved by the NDB before implementation and should be tested before going live.
- Handover of the system to respective teams in NDB should be completed with training and documentations before completion of the project
- The solution or system should provide the at least 4 platform dev/UAT, prod and BCP which is continuously tested and usable as per the requirements from the NDB
- The final sign off of the implementation will be given post production go live and sign off from the project team in NDB.

Security:

- The Implementation to adhere to the signed off users roles and access control as per the NDB Security requirements
- The solution or system needs to be tested for the industry standard information security parameters and should have inbuilt self-auditable security testing mechanism.

Documentation and training:

- Full manual on using the solution and system
- Training for the Bank's staff for the administration, configuration, changes, business use cases etc. and should be signed off by concerned teams and users
- Initial period of maintenance and troubleshooting, identified non-conformity for the period post implementation and handover to be 6 months

Attachment 2:

Information Category	Description	Supplier's inputs
General Information	Legal Entity Name	
	Legal Address	
	Website	
	Government Registered Number	
	Date of Registration	
	Tax ID	
	Name(s) of Authorized Signatory	
	Contact Information (name, title, mail address and telephone number)	
	Amount of Employee	
	Three reference customers for Similar case(minimum)	
Financial Information	Registration capital	
	Revenue of last 3 years	
Other Information	Information Security Credentials if any	
	Data residency location, for providing service required in the RFP	
	IDD/ AML Sanctions, Yes or No. If yes, please specify.	
	Others deemed necessary	