1. Expression of Interest

EOI Title: Integrated Risk Management Implementation

New Development Bank (NDB or the Bank) intends to implement Operational Risk Framework on ServiceNow integrated Risk Management for its IT Setup for Risk Division's Enterprise and Operational Risk Unit. Please provide feedback with regard to information and quotation according to the requirements in this document

2. Time

Please feedback this request within 7 days
The minimum validity of the quotation should be one week.
The response to the RFI should include fees for each of the requirement line items and Implementation effort in mandays.

3. Method of submission

a. The technology details, checklist for technology etc. with EOI Title to be submitted to sonbhadra.saurav@ndb.int

b. Quotation to be submitted with EOI Title as password protected files to siva.srinivasan@x.ndb.int

c. Passwords to be communicated with EOI Title to

i. Alexander Baryshnikov – Chief IT – New Development Bank baryshnikov.alexander@ndb.int

4. Technical specifications

The proposal needs to cover the high level checks on following Scope of Items, however, the same is not limited to the below mentioned categories. NDB Intends to have the implementation carried out as per the internal standards, established & relevant industry standards, preferably with pre-loaded risk libraries(e.g. COSO ICF, COBIT, etc.). The expected outcome should be feasible, implementable, align with technical strategy and can be validated and audited for the framework to cover the standards implementation.
The table below summarizes the key functional modules needed to be configured on the solution to drive the risk management activities:

Module	Functionalities/ features
Risk & Control Library/ Risk and Control Self-Assessment	• Documentation of list of Business Units, Products, processes, sub-processes/activities • Documentation of risks (What Can Go Wrong), mapping to processes/sub-processes.

Module	Functionalities/ features
	• Documentation of Controls for each risk. • Mapping of multiple risks to multiple controls should be enabled; • Standard characteristics for risks and controls should be available • Basel loss event categories, customizable business lines mapping feature should be available; • RCSA methodology should support inherent risk scoring for risks (likelihood and severity) and control effectiveness scoring and arriving at residual risks • Control types/features should be available (like preventive/detective, automated/manual, operating effectiveness, etc.) • RCSA planning, and workflow should be strong - assignment of users, defining user roles, alerts, etc.
Control Testing	• Controls testing features as mentioned under RCSA section should be available; • Controls features should confirm to standard frameworks like SOX framework. • Issue assignment and tracking
OR Incident management	• OR Reporting template – OR Losses and near misses (as per Bank's internal reporting requirements – Basel loss categories) • Workflow (reporting, approval, monitoring) • Accounting: Loss, recovery and write-off • Issue tracker
Key Risk Indicators (KRI)	• Library configuration (definition, metrics, thresholds) • KRI types and features should cover features like lead indicators, lag indicators, key control indicators, key risk indicators, etc. • Features for assigning tolerance limits • Data input: time bound notifications, escalations & automated data collation (other systems) • Reporting • Issue tracking • Facility to link incidents to RCSAs and KRIs.
Reporting	• Dashboards – OR team and OR champions (Division specific) • Consolidated action points reports

Module	Functionalities/ features
	• Automated reporting, triggers
Vendor risk management	• Vendor risk assessment methodology; • Vendor criticality assessment and assignment • Facility to fetch vendors base data from base vendor module (NetSuite system) • Vendor reviews planning and reporting • Strong reporting generation •
Cybersecurity & Cloud risk Assessment	• Cybersecurity assessments and risk planning; • Pre-loaded standard like NIST cyber security framework. Provision to assess and monitor compliance to framework; • Cloud risk assessment templates (for on-boarding cloud service providers, on-going monitoring and periodic risk assessments); • Pre-loaded Cloud Security Alliance standard to check and monitor compliance to framework; • Templates & Questionnaire; • Strong reporting mechanism, issuance and action tracking.

5. Service specifications

- **Integration with the framework libraries**
- **Customization of the framework for the approved controls**
- **Controls lifecycle automation**
- **Integration with ITSM and Monitoring**
- **Integration with other modules**
- **Integration/ APIs/ ability to obtain risk related information from Bank's prevailing systems**
- **Service providers should have at least 4 Banking industry experience for the in-depth implementation of Integrated Risk Management**
- **Should be able to record and transition all configuration to the SNOW team**
- **Post implementation support for the stabilization period**
- **Training and Handover**
- **Formulation for access on Mobile apps**
- **Automation of modules as required**

Contacts

6. **Technical queries other than commercials terms, if any shall be addressed to the following contact:**
   Mr. Saurav Sonbhadra, sonbhadra.saurav@ndb.int.

7. Responding to this Expression of interest does not constitute any contractual obligation and rights on the part of the vendor.

   Please provide the expected time line for completion of Implementation