Request for Information

1. Introduction

New Development Bank (NDB) requires Identity Governance and Administration tool. Please feedback the information and quotation according to the requirements in this document and attached IT questionnaire.

2. Time

Please feedback this request by December 12th, 2019.
The minimum validity of the quotation should be one week.
The response to the RFI should include fees for each of the requirement line item.

3. Method of submission
    a. The technology details, checklist for technology etc. to be submitted to sonbhadra.saurav@ndb.int
    b. Quotation to be submitted as password protected files to gu.qinghua@ndb.int
    c. Passwords to be communicated with subject line of the product to
        i. Alexander Baryshnikov – Chief IT – New Development Bank baryshnikov.alexander@ndb.int

4. Technical specifications

The Identity Governance and Administration tool and services needs to meet the following requirements. The minimum support and unit pricing can start from 200 users. Preferably hosted on SaaS service ServiceNow.

1) **Scenario 1.** User access request (self-service)

    - Users on their own behalf request access with the following parameters
      - System
      - Role in the System
      - Expiration date
    - Line manager (or deputy) approves with optional possibility to change expiration date (not more than mandatory recertification period). Verification against SoD and other Policies.
    - Business System owner (or deputy) approval.
    - Access implementation (automatic or manual).
    - The set of users to be catered is 200 at present internal and around 500 for external.

2) **Scenario 2.** Access certification (auto triggered)

- When expiration date approaches (e.g. two weeks or one month before expiration), Line Manager and his deputy receive automatic request for User access certification.
  - System
  - Role in the System
  - Expiration date
- Line manager (or deputy) either confirms User access with optional possibility to change expiration date or revoke all or any specific system access.
  If LM does not make a decision, User's access is expired and to be revoked by Scenario 4.
  Verification against SoD and other Policies.
- Business System owner approval.
- Access implementation (automatic or manual).

3) **Scenario 3.** Access revocation

- Authorized person (e.g. HR, line manager, business system owner, IT Security etc.) raises request for access revocation with parameters
  - User
  - Specific System or ALL systems
  - Role in the System
- Access revocation implementation (automatic or manual).
- No approval is required.

4) **Scenario 4.** Access expiration

- On expiration date (if access was not confirmed) access is revoked automatically or admin receives notification for manual access termination.

5) **Scenario 5.** Access revocation triggered by HRMS

- Access revocation for all system if employee contact is marked as closed in the HR management system.

6) **Additional requirements**

- Access change log with automatic notifications.
  Dashboard, Compliance and Audit reports.
- Report which compares granted access rights with actual permissions in business system.
- Any Integration activity between AD and O365
- User access request (self-service)
- Access certification (auto triggered)
- Access revocation
- Access expiration

- Access revocation triggered by HRMS
- Integration with in-scope applications (using out of box connectors)
- BambooHR as HR management system (Source of Truth)
- NetSuite (Basic connector)
- OKTA
- AD
- O365 (China)
- Configuration of Reports (out of box reports)
- Access change log with automatic notifications
- Dashboard, Compliance and Audit reports
- Access reconciliation (Report which compares granted access rights with actual permissions in business system)
- Should be self-maintainable and requires least management overhead. Should be manageable by Customer end
- Configuration changes, application addition etc. can be end users without much of code
- Out of the box rest api support for major SaaS vendors
- Out of the box support to create new integration through rest APIs
- Out of the box Integration to ServiceNow, Okta, Privilege Access Management solution etc.

5. Service specifications

- The service provider is able to host it as SaaS within the BRICS nations
- The service provider is able to run it as SaaS 24*7*366/365
- The supplier is responsible for device setup and deployment according to NDB requirement.
- During the device maintenance period, the supplier provides NDB Shanghai Office 7*24*4 on-site and remote service in case of NDB request.

6. Contacts

Please feedback to the following contact:
Mr. Saurav Sonbhadra, sonbhadra.saurav@ndb.int.

IT_Risk_Questionnaire- This section-Please download and reply in excel format

Requirement Item	Requirement ID	Short Description	Long Description	Out of the Box /Customization (Simple/Medium/Complex and no. of Mandays)	Explain (As applicable, May share the attachment)
19.0 IT Architecture	**19.1**	Technical Architecture	Details around each components (preferably a diagram) around each modules.		
	19.2		Technology Stack Architecture (Program/Development-J2SE, Fusion Forms, Spring Based, proprietary languages if any, platform stacks - webservers, applications servers, databases, reporting, backup/ replication etc. used and supported).		
	19.3		No of host Servers		
	19.4		Amount of storage		
	19.5		Configuration of Hosts		

	19.6		Platforms hosted on each Hosts (Web server, Clients (if applicable), Connections, Load Balancers/ADCs, Middleware's, Databases, Messaging layers, Caching layer, Rule Engines etc.		
	19.7		List all the app instances and respective modules they are supporting on each level and hosts including the load balancers and ADCs		
	19.8		What are the expected number of Infra and Core Components from Bank, if hosted in SAAS , explain expected number of infra and hosts used as explained above		
	19.9		If hosted in service provider facilities can we ensure the site-site vpn/ firewalled at L2 and above layers , connectivity to entire stack exclusive to NDBs solution environment and the access		

			governance be controlled by NDBs systems		
	19.10	Deployment Architecture	Deployment architecture- Monolithic, Multilevel, SOA (mention percentage of code as service oriented with modules and API list), Micro services (how is the implementation done, name the services and modules it overs)		
	19.11		If microservices architecture what is the service discovery mechanism, can u share the CI/CD components being used and the pipeline and antifactory repositories. Can the mirror be setup as well in NDB's facilities.		
	19.12		Minimum number of VMs/servers/containers required for High availability mode.		

	19.13		Specify the details on UI+Application Logic +Database layers flow architecture with ports and certificates interaction if applicable.		
	19.14		User Interface (UI) is it Browser based or Thick Client Based		
	19.15		If Thick client based , share the technology used Java/.Net/Fusion Forms etc.		
	19.16		What is the distribution mechanism of thick client with updates and changes. How will it be distributed to end users. How can end user connect to thick client Cover that as part of the architecture		
	19.17		What is the pre-requisite for thick client installation- runtime , dependent libraries etc.		
	19.18		If Browser Based , what is the underlying technology, is it HTML , Which Version of HTML , CSS (Is it adaptive CSS		

			UI), Angular JS, JavaScript, React etc.		
	19.19		Do you need ActiveX/com specific version of JRE/.Net runtime components for the UI to be working on browser		
	19.20		What is the mechanism to handle last known user data and session , does it throws http error in case of next layer not available?, how does it present the data back to user and default message for user.		
	19.21		Does the solution uses users temp data or session details caching . Through Client side browser of server side scripting.		
	19.22		Can the application be deployed in containers or VMs?		

	19.23		Can solution be hosted as a whole as Software as a Service in our Virtual Private Cloud (VPC) in Ali Cloud Hong Kong and Mainland or Azure China? Pls specify		
	19.24		What is the replication mechanism used for application updates to primary and DR site- manual deployments, app/web server deployment manager such as WebSphere etc., additional internal logic.		
	19.25		What is the replication mechanism for databases , intrinsic to database , storage level , third party tools , pls explain.		
	19.26		Level of interfaces available for applications eg: messages based, rest APIs, web services etc.		
	19.27		Flexibility and Feasibility of changes. Quickest turn around for any change, without		

			impacting other modules/interfaces?		
	19.28		How does solution ensures zero-downtime or impact for database upgrades / patches (including kernel patch etc), Middleware (VA patch etc) , changes to app impacting databases, schema, stored procedure changes etc., eg: do you use dual schema updates and schema based reverse mirroring or schema changes?		
	19.29		Does the application make use of in memory + disk write/read first or message queuing to ensure caching and replay of transaction in case of underlying component unexpected unavailability? Pls explain		

	19.30		Data storage format being supported such as relational, columnar, hierarchal, Jason, proprietary xml etc. and for which application modules?		
	19.31		If hosted in virtual private cloud, which all Platform as a Service (PaaS) capabilities can we leverage securely?		
	19.32		Does the solution uses load balancers and ADCs ? Can the application support local as well as site level load balancing?		
	19.33		If the solutions uses ADCs what are the functionalities of ADCs used SSL offloading, compression, acceleration, caching etc.		
	19.34		If the solution is hosted in service providers own facilities and offered as a service , can we deploy active-active setup in NDB's controlled environment and		

			complete sync with the data and information at any point in time.		
	19.35	Access Management and Security	Is the complete control of Identity and access management be done through integration through NDBs IAM/IGA system , including support for MFA ?		
	19.36		Can the software expose the APIs or Read only access to all authorization schemas/objects and their respective audit logs to integrate in back to Banks IAM/DW solution.		
	19.37		Can the authorization and access management for the application be controlled, automated and modified through IAM solutions		

	19.38		Integration with SSO in place? Supported SSO and SAML version?		
	19.39		Level of encryption with data at rest, data in transmission and decryption management in process data. Version of SSL and encryption mechanism SHA2 , TLS 1.2 etc		
	19.40		Level of encryption with user access to UI, UI to app and all to DB and DB to backup/restoration. Level of secured hand shake provided with Interfacing applications.		
	19.41		Can solution support complete encryption management Key center outside the application environment with password vaulting and management for all users' credentials, including the service user for connection, running and deployment of applications components from		

			outside application environment.		
	19.42		Are there unique features to ensure secure access, storage, transmission, process, backup/recovery/replication and audit log for the same.		
	19.43		Has the application been tested for cross site scripting		
	19.44		Can report be provided on Independent VA/PT done post implementation		
	19.45		Can report be provided on Independent Cross Site Scripting done post implementation		

	19.46		Can report be provided on Independent SQL Ingestion test done post implementation		
	19.47	Log Management, Error Handling and Incident Generation	Self-monitoring and alert generation and integrated reporting in bank's incident management system.		
	19.48		Level of log generation applications level and database levels application flow event logs for each activity - Audit trail logs for vetting the flow and raising incidents if any error. Application logs for all error and internal faults and accordingly report incidents Integration to bank hosted incident, change , service and problem management system.		
	19.49		Is logging enabled for User Interface, Application, Database any other components. Pls specify what is not covered		

	19.50		Is the Audit Log enabled for all the components		
	19.51		Is the error logs enabled for all components		
	19.52		Is there any other critical application thresholds being logged such as simultaneous users, authorization failures etc.		
	19.53		Pls mentions the components which are not being logged		
	19.54		Does the application alerts on the probable failure basis error handling/other logs		
	19.55		Can the systems at all levels generate the incidents and can it be integrated back to NDBs Incident management system		
	19.56		Are there any restrictions to following NDBs Change management standards and process , with integration through NDBs change management systems		

	19.57		Can the system be integrated to discover the CMDB information for each component and feed in back to NDB ITSM solutions. Are there any restrictions		
	19.58		Error handling- How does system handles error reporting and handling. Can all error be reported through incident		
	19.59		Can the audit logs on the application and/or databases be traced back to the transaction flows to establish any potential operation risk.		
	19.60		Does application holds capability to simulate or replay a transaction		
	19.61		Can application be integrated to Monitoring tools such as Appdynamic, Real user Monitoring, Profilers out of box and exposes to log and capture issue out of the box		

	19.62	Infrastructure to manage availability, reliability, change and scalability	How does application manage availability, reliability, change and scalability? Does it depend on the Infrastructure components to deliver the same or are there unique capabilities please share?		
	19.63		How UI sessions are maintained in HA mode, is it sticky session, caching of session, stateless session and cached at webserver end? How to recover session in case of local failover , how is session redirected .		
	19.64		How is application session maintained, is it per user session based , how do we recover in case of failure. How is database sessions recovered from failure and how are the transactions replayed.		
	19.65		Can the application be hosted and orchestrated using containers.		

	19.66		Are we using database HA features such RAC /Always on/ SHRAD , Pls explain.		
	19.67		Can database connected with service names and on common load balancers with distributed databases?		
	19.68		How is the application/web and databases backed up		
	19.69		Can solution support snapshost based recovery at web and application layer		
	19.70		Can solution support immutable data for the archive and backup		
	19.71		Can the data be backed up and recovered point in time		
	19.72		Can solution application disaster recover in automated way, do you provide run books from recovery or needs integration to automated solution, third party? Pls explain		

	19.73		Can solution load balance and run Active-Active setup or only active-passive is supported? Explain at which levels		
	19.74	Integration	List the web services, APIs according to the modules , forms and fields- Pls specify specifics to each modules/forms and fields		
	19.75		Pls include input and output of the APIs (particularly if it offer JSON,XML as an output)? Pls elaborate on each APIs input and Output and the associated application/database modules.		
	19.76		Can solution integrate to Outside BPNM Engine ? What is the available option		
	19.77		Does solution exposes APIs or Message based communication to other platforms		

	19.78		Can the application entries and flows be integrated to other application as the starting point of flow initiation for any process.		
	19.79		Can we eliminate all manual inputs to the application through External BPM and Application interaction		
	19.80		Can the application and database be integrated to NDB's DataWarehouse for all data		
	19.81		Is the service provider solution is compliant to standards such as NISC/PCI DSS - can details be provided		
	19.82		Does solution has any restriction to support standard EAI platform, such as Redhat Fuse ,MuleSoft , Dell Boomi etc.		
	19.83		Can solution make use of messaging queue in		

			terms of AMQ , IBM MQ , WebLogic JMS etc.		
	19.84		Pls explain can solution run and integrate with web services independently and can it be scaled independently, without any customization.		
	19.85		What are available format for reporting, can the reporting be fed back to another systems using any format such as Jason/XML etc. and be integrated to BPM workflow outside the solution for integration to other applications. Can it be done through any application API.		
	19.86		Can it be integrated with Enterprise content management if required through enterprise integration platform		

	19.87	Demographic/Legal/Compliance	Are there any restrictions in terms of the compliance to own, store , share , comply with data and information governance from countries outside BRICS nations		
	19.88		If yes can you remove the clause or provide any alternative		
	19.89		Which countries laws/regulation takes precedence and applicable for the solutions/data/information- Is it Hosting countries/Customer or the Country of Origin or Head Quarter		
	19.90		Where will all the components be hosted if not in NDB preferred location, how is the integration planned. Complete control and availability of Data and Information is ascertained to NDB alone ant any point with or without the software ?		

	19.91	UI and Testing Covered	If application browser based. Is Application tested for all browser ? If not name the browsers supported		
	19.92		If application is thick client based what end user deployment mechanism, have we tested for remote session/ blurring etc.		
	19.93		Can you carry out a testing against all scenarios functional post UAT deployment		
	19.94		Can you carry out negation testing against all fields		
	19.95		Can you carry out a blackbox testing for application once deployed and submit a report		
	19.96		Are there readily available automated test scripts and images to host the test script/test cases for validation of all fields, flows, exceptions, errors and negation out of the box.		

	19.97	Data Management and Governance	Is the database recommended is RDBMS/Distributed/In-Memory/Hierarchal/ Columnar- Explain the combination as applicable		
	19.98		Does the solutions utilizes In-Memory read and write of data		
	19.99		Does the solution utilizes In-Memory at DB end or application end		
20.0 Solution/Security/database	**20.1**		Can you list all the schemas of database , with their respective modules in application		
	20.2		Do you support zero downtime database upgrades and kernel patching		
	20.3		Do you support Zero downtime solutions upgrade with rollback the application and schema/objects changes		

	20.4		Are there mechanism to have different schema for Access /Authorization, Master Data, and Transactional data segregation encrypted using different keys.		
	20.5		Do you use database links for inter database and schema interactions		
	20.6		Do you support encrypted database		
	20.7		Has the database been tested against SQL ingestion		
	20.8		Can the DB admin account be password vaulted and integrated through the NDB IAM/IGA solution for authorized access and audit logging		
	20.9		How is database connected JDBC/ODBC third party drivers, pls mention and explain		
	20.10		Can we create read only accounts for the database and for all		

			schemas and data. Pls explain the exceptions		
	20.11	Governance/reporting	Whether CSP will publish any report/dashboard is prepared and published by CSP on a periodic basis? To cover performance metrics. (e.g. uptime/downtime; incidents; changes; bugs; transaction volumes; etc.) - for the services used by NDB		
	20.12	Data Management	Which practices are followed by the CSP for protecting the NDB data from other clients' data? Is there a logical or physical partitioning of data?		
	20.13	Data Environment	Data centers location of CSP (as well as DR center) where NDB data will be stored (either main data or back-up data) in non-BRICS countries? Whether cross border data		

			migration is possible without NDB's approval?		
	20.14		Whether CSP facilitates to back up NDB data on NDB's premises/ in NDB's data center?		
	20.15		What is the data extraction mechanism when software has to be withdrawn?		
	20.16	Cyber Threat	Whether CSP is having a comprehensive Security Patch and vulnerability management programme? High-level details of the process followed?		
	20.17		Whether CSP is having a comprehensive Security Monitoring mechanism? High-level details of the tools and process followed?		-

	20.18		Whether regular penetration tests are carried out by CSP? Whether NDB could apply our own penetration test?		
	20.19	Infrastructure, change management	Whether CSP is having a comprehensive change control mechanism for the cloud provider infrastructure, such as system patching, firewalls, intrusion detection, anti-malware, virtual environment management, and hardware equipment?		
	20.20		Whether CSP is having a robust SDLC process, change notification and release management process of CSP? (pertaining to NDB system / service)		
			Physical security measures of data centers (primary and DR centers, where NDB data is located) adopted by CSP?		

	20.21	Logs and Audit Trails	How long are logs and audit trails kept by the CSP pertaining to software used by NDB and data of NDB; whether these are available for access by NDB?		
	20.22	Availability	Whether the CSP will agree upon the uptime tolerance prescribed by NDB and incorporate in Service Level Agreement (SLA)? What has been the actual uptime level in the last 12 months of the Software offered by CSP?		
	20.23		Does the CSP have resiliency (e.g., cluster systems, redundancy, and failover capabilities) and tests these abilities after changes or system updates?		
	20.24		Does the CSP have an incident response plan? What are the major incidents in the last 12 months? Whether NDB will be informed and within what time?		

	20.25		What measures are employed to guard against threat and errors and denial of service (DoS) protection, by the CSP?		
	20.26		When do "peaks-in-demand" occur, and does the CSP have the capacity to handle such maximum load?		
	20.27		Whether CSP will offer services under Disaster Recovery/ Business Continuity conditions, will these be incorporated in SLA?		
	20.28	Identity and Access Management	Whether third-party or its staff has access to NDB data? What are the control processes for Third-party access to NDB's data, at CSP end?		
	20.29		Application security controls for cloud provider staff and audit - whether CSP has implemented Identity Access Management solution? Is there a policy for role-based		-

			Segregation of Duties (SOD) for granting access to system?		
	20.30		What types of access is practiced by CSP: single-sign-on (SSO), authentication using the client identity management software, or two-factor authentication?		
	20.31		Whether IP restriction for access will be supported by CSP?		
	20.32	Encryption	Whether NDB data stored on CSP's servers is encrypted? Whether back-up data is also encrypted?		
	20.33		Is there any encryption mechanism/software used for data at rest?		

	20.34		Which kind of encryption software used by CSP? SSL should provide a minimum of 128-bit, 256-bit optimum, encryption based on the 2048-bit global root. Determine the type of encryption.		
	20.35	Privacy	Can the CSP provide full details of data of NDB which will be stored by CSP?		
	20.36		Whether critical data of NDB will also be accessed by third-parties/government agencies?		
	20.37		Whether CSP is governed by any of the regulatory or statutory guidelines? Whether CSP will share NDB data with hosting country agencies or other countries)?		
	20.38		Whether CSP is certified for SOC 1 and/or SOC 2?		
	20.39	Legal	Whether CSP will agree to include the following clauses in the Service		

			Level Agreement for software :		
			- Right to Audit and physically inspect;		
			- Timely removal of data and destruction;		
			- Change control notifications;		
			- Uptime/availability metrics under normal and DR/BCP scenarios;		
			- Data privacy, confidentiality, backups;		
			- Prior approval for sub-contracting services to other vendors;		
			- SOC 1 or SOC 2 certifications, maintenance and renewal;		
			- Data storage locations;		
			- Penal clauses;		
			- Escrow arrangement		
	20.40		Are there certain scenarios whether CSP can unilaterally block or terminate the services/contract (other		

			than payment related issues, if any)?		
	20.41		Whether CSP can levy any additional fees for termination of services, delivery, or erasure of data or penal clauses; also check notice period.		