New Development Bank

Request for Proposal

(This is not a Purchase Order)

1. Introduction

New Development Bank (NDB) is issuing a Request for Proposal (RFP) to invite qualified suppliers to provide proposals for NDB's **Information Technology & Security Governance, Policy & Procedure Consultancy Project**. Please refer to the following information and attachments for detailed requirements.

Each interested party must submit their proposal in response to this RFP to the contact person listed below by **Sep.8, 2023, 5:15pm CST.** NDB will appoint the service provider in accordance with internal policies and guidelines. NDB at its sole discretion reserves the right to reject proposals in accordance with its internal policies and guidelines.

2. RFP Schedule

Please note that the following activities would 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	Aug. 11, 2023
Deadline for questions if any	Aug.18, 2023
Proposal Response Due	5:15pm CST Sep.8, 2023
Signing Contract	TBD
Project Kick Off	TBD

3. Instruction to bidders

3.1 Contact Information

Please use the following contact information for all correspondence with NDB concerning this RFP. **Suppliers who solicit information about this RFP either directly or indirectly from other sources will be disqualified.**

Contact Person:
Ms. Holly Yao
Address: NDB Headquarter, 1600 Guozhan Road, Pudong New District, Shanghai, China
上海市浦东新区国展路 1600 号，新开发银行总部大楼
Email: yao.holly@ndb.int
Tel: +86-21-8021 4489

3.2 Submission of Proposals

Proposals shall be in English. Both hard copy and electronic version is acceptable. Hard copy (6 copies at least) shall be sent in sealed covers and addressed to the contact person. Electronic version shall be sent with protection (at least with a password).

The mentioned deadline, due time, closing date, etc. herein means Beijing time (CST) and during NDB's business hours from 9:00AM to 5:15PM on weekdays.

3.3 Questions

Questions should be submitted in writing by e-mail. Prospective vendors should refer to the specific RFP paragraph number and page and should quote the questioned passage. NDB will be prompt in responding to communicated questions.

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 prospective vendors.

3.5 Proposal Costs

NDB is not liable for any costs incurred by the prospective vendors in the preparation and/or submission of the proposal.

3.6 Proposal Format (Suggested)

NDB recommends that the proposal should contain the following (at minimum):

Volume 1 – Main Proposal

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

Volume 2 – 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 for a period of at least _90_ days.

3.8 RFP Amendments

New Development Bank reserves the right to amend this RFP any time prior to the closing date. In the case of such an event, prospective bidders will be notified, and amendments will be issued only to those prospective vendors with intent to complete a proposal for submission to NDB.

3.10 Award Notification

NDB may negotiate with all shortlisted prospective vendors before deciding on the winning vendor. NDB reserves the right to negotiate further with the winning vendor before and in the contracting process. The remaining vendors will be notified in writing of their application status.

4. Evaluation Criteria

The proposals will be reviewed and evaluated by NDB's team in accordance with the related policies and guidelines on the six principles of Economy, Efficiency, Competition, Transparency, Value for Money, fit for Purpose as contained in NDB's corporate procurement policy. NDB is interested in obtaining a complete solution for the requirements contained in this RFP. Sub-contracting is not permitted. 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 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. Prospective Vendors 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, prospective vendors must demonstrate adequate experience in developing and implementing the requested project. NDB's confidence in the vendors' ability to meet deadlines and successfully manage similar projects will be a primary consideration.

Special consideration would be given to vendors 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 vendors will be carefully examined. Price will be used as a final indicator for determining the vendor finalists when all other criteria have been normalized.

iv. Presentation and Demonstration

Presentations and Demo's provided by prospective vendors will be considered and evaluated.

v. Support and Maintenance

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

New Development Bank

Project Terms of Reference

Project:	**Information Technology and Cyber Security Process and Governance Consultancy Service**
Owner:	**Information Technology Division**
Version:	**V1.0**
Date: [●]	**17/07/2023**

Project Background

Overview

This project aims strengthen the overall Information Technology and Cyber Security governance, management, control and procedures via the following activities supported by an external consulting firm:

- Review and develop the required policies, guidelines and procedures in accordance with industry best-practices frameworks and the business reality of NDB.
- Recommendations of architecting and implementing these processes and policies organizationally and systematically.
- Review and recommend other necessary process definitions which are not covered in the current governing system or the requirement in this document.

Project Constraints

The standard service is at NDB HQ working hours. Interviews and information gathering requires previous date/time agreements and availability. In some cases, availability might change due to unexpected events.

Objectives

Main Objective

- Establish policies and procedures based on industry related frameworks (ITIL, COBIT, CMMI, ISO38500, etc.).
- Establish policies and procedures based on industry related frameworks (NIST, ISO, HIPAA, etc.).
- Review, update and streamline IT policy document hierarchy.
- Review, update and streamline Information and Cyber Security policy document hierarchy.

Intended benefits.

Strengthen the overall Information Technology and Cyber Security governance, management, control and procedures.

Project Scope

Information Technology Scope:

- Information Technology Process and Governance Documents to be developed:
    - Develop a Service Provider Management guideline**.**
    - Develop an asset management guideline.
    - Develop a software development management procedure.
    - Develop a service configuration management procedure.
    - Develop a Network Operation Centre (NOC) operation procedure.
    - Develop a System and Application Integrated Operation Centre procedure.
    - Develop a service monitoring and log management procedure.
    - Develop a system and data integrity management guideline.
    - Develop an end-user device application management guideline.
    - Develop a knowledge management procedure.
    - Develop an IT service supply chain management procedure.
    - Develop IT technology architecture procedure.
    - Developing an electronic data retention guideline
- Information Technology Process and Governance Documents to be reviewed and updated:
    - Review and update Information Technology Policy and Service Management Policy
    - Review and update IT project management guideline.
    - Review and update IT service management policy and IT Operations Management Procedure.
    - Review and update IT change management guideline.
    - Review and update IT incident management guideline.
    - Review and update IT problem management procedure.
    - Review and update IT Service Continuity Guideline (disaster recovery management guideline)

Information and Cyber Security Scope:

- Required Information and Cyber Security Policy, Process and Governance Documents:
    - Develop Identity and Access management (Logical access management) guideline.
    - Development a Security Awareness and Training procedure.
    - Develop Cyber Incident & Response Management guideline.
    - Define Threat Intelligence procedure.
    - Define of a Data Leakage and Protection guideline.
    - Developing Bank wide Data Classification guideline.
    - Develop Digital Certificate and Encryption Key Management procedure.
    - Develop Cloud Service Security Management procedure.
    - Develop Security Penetration Test and Remediation procedure.
    - Develop a KPI standard for information security.
- Information and Cyber Security Policy, Process and Governance Documents to be reviewed and updated:
    - Review and update Information Security Policy.
    - Review and update Data Leakage Prevention guideline.
    - Review and update Privileged Access Management procedure.
    - Review and update Vulnerability Management procedure.
    - Review and update Information Security Operation Centre procedure.
    - Review and update IT system baseline and hardening standard

Outputs / Deliverables

- Policy, guidelines and procedure documents that are approved by the concerned authorities in the Bank.

Resources Required

- All project stakeholders
- Solution provider

Methodology

Project Phases

- Initial request
- Terms of Reference (this document)
- Requirements
- Procurement
- Contract
- Implementation
- Post implementation support

Project Activities

- Initial Request and Review
- Project Terms of Engagement
- Requirements Gathering
- Proposal Request, appraisal, and contract signature (Corporate Procurement)
- Implementation
- Business acceptance
- Post Implementation Support
- Project Review

Analysis Tools

- Project reports.

Project Plan

Project Timeline

Activities	Description	Responsibility	Timeline (Tentative)
Initial Request and Review	Identification of needs which translates to a requirement for an IT function or service	IT PM & Business Sponsor	Week1
Project Terms of Engagement	This is a formal process that documents the agreed scope, extent, and deliverables of the project, as well as the project roles and responsibilities, in a key project document.	IT PM & Business Sponsor	Week1
Requirements Gathering	During the Requirements Gathering process, as much uncertainty as possible is removed, and a baseline is established. Any change to the requirements after the baseline is established is subject to change control.	IT PM & Business Analyst	Week2
Proposal Request, appraisal, and contract signature	Activity initiates Corporate Procurement, review of SOW, Final SOW from all stakeholders sign off	Corporate Procurement	Week 3-7
Implementation, Configuration & Handover	Actual Production Transition	Business Analyst, Service Provider, and IT PM	Week7-22
Business Acceptance	Accept on solution delivered	Business Analyst and Sponsor	Week22-24
Project Review	Project Review for the outcome of the project activities and open tasks. Leads to Phase 2	Ongoing with IT Project Managers and Business Partners	Week24

Reporting

Project Schedule Tracker/Milestone Report

NDB Information and Cyber Security
Process and Governance Consultancy Service
Requirements Specification

Version 1.0
2023.07.06

Executive Summary

Project Description

This project is to request information and cyber security process and governance consultancy service to:

1. Review and develop the required policies, guidelines and procedures in accordance with industry best-practices frameworks and the business reality of NDB.
2. Recommendations of architecting and implementing these processes and policies organizationally and systematically.
3. Review and recommend other necessary process definitions which are not covered in the current governing system or the requirement in this document.

Functions and Features

Functional Requirements

Functional requirements define the features the service must provide.

1. General requirement to the consulting team
    - Expertise and Experience: The consulting team should have a strong background and extensive experience in Information and Cyber Security management, governance, technology, and operation. They should possess deep knowledge of industry best practices, frameworks (such as NIST, ISO, HIPAA, etc), and regulatory requirements related to Information and Cyber Security, especially the financial industry and MDB (multilateral development bank) community.

    - Relevant Skills and Certifications: The consulting team should have a team of consultants with the necessary skills and certifications. This may include certifications such as CISA, CISM and/or CISSP.

    - Understanding of Organizational Context: The consulting team should demonstrate a strong understanding of NDB's organization, industry, size, complexity, and specific Information Security management and governance challenges. They should be able to align the recommendations and solutions with NDB's context and strategic objectives.

    - Methodology and Approach: The consulting team should have a structured and proven approach for conducting assessments, developing policies and frameworks, and implementing governance structures. This ensures a systematic and effective engagement.

    - Collaboration and Communication: The consulting team should demonstrate excellent communication skills, actively listen to NDB's needs and requirements, and foster collaborative working relationships with project stakeholders.

    - Tailored Solutions: Look for a consulting team that can provide tailored solutions to meet your specific needs. They should be able to customize policies, frameworks, and governance structures to align with NDB's culture, processes, and industry regulations.

    - Project Management and Timelines: The consulting team should have a track record of delivering projects on time and within budget, proven project management methodologies, deliverable milestones, and reporting mechanisms to ensure effective project oversight and transparency.

    - References and Reputation: The consulting team should have high reputation in the industry with testimonials, case studies, or client success stories that demonstrate their ability to deliver value and achieve desired outcomes.

    - The consultant team should support the clarification and necessary revision of the defined and revised policies, guidelines, and procedures through NDB internal review and approval.

2. General requirement to the policies, guidelines, and procedures to be developed or updated.
    - Establish policies and procedures based on industry related frameworks (NIST, ISO, HIPAA, etc) and and cross match to ensure the completeness of principles of the frameworks adaptable to NDB are in place.
    - Review, update and streamline Information and Cyber Security policy document hierarchy.

- Guideline document has its direct impact and requirement to IT and other business units, which Procedure document are mainly for IT internally.
- Foster a culture of continuous improvement of the related process. Regularly review and evaluate the effectiveness of the process, seek feedback from stakeholders, and implement improvements to enhance efficiency, minimize risk, and improve overall service delivery management and quality.
- Compliance and Reporting: Ensure that the policy, guideline, and procedures comply with applicable industry and internal regulation and requirements.
- Provide training and awareness programs to relevant stakeholders, including IT staff and end users, to educate them about the related process, roles and responsibilities, and the importance of reporting promptly and accurately. This helps ensure consistent understanding and adherence to the regulatory document.
- Define metrics and key performance indicators (KPIs) to measure the effectiveness and value of the defined guidelines and procedures.

3. Required Information and Cyber Security Policy, Process and Governance Documents
   - Develop identity and access management (Logical access management) guideline.
     - Draft processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including review of access granted to third-party provider. All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.
     - Policy Framework: Develop a comprehensive policy framework that outlines the organization's IAM objectives, roles and responsibilities, and compliance requirements. This framework should align with industry best practices and internal regulatory requirements.
     - Access Control: Implement strong access controls to enforce the principle of least privilege. This includes defining user roles, granting appropriate access rights, and regularly reviewing and updating access privileges based on job functions and changes in personnel.
     - Authentication: Establish secure authentication mechanisms to verify the identity of users accessing the organization's systems. This may involve the use of strong passwords, multi-factor authentication (MFA), biometrics, or other advanced authentication methods.
     - Authorization: Define clear authorization rules to determine what actions users are allowed to perform within the system. Role-based access control (RBAC) is commonly used to assign permissions based on job roles and responsibilities.
     - User Provisioning and De-provisioning: Implement a process for efficient user provisioning when onboarding new employees and contractors. Similarly, establish a robust de-provisioning process to revoke access promptly when individuals leave the organization or change roles.
     - Segregation of Duties (SoD): Enforce separation of duties to prevent conflicts of interest and minimize the risk of fraud. Users should not have conflicting responsibilities that could lead to unauthorized access or fraudulent activities.
     - Monitoring and Auditing: Implement monitoring and auditing mechanisms to track user activities, detect unauthorized access attempts, and identify security incidents.

   - Development a security awareness training procedure
     - Draft information security awareness program in line with the organization's information security policies, data privacy policy and relevant procedures. 1. New hire orientation, 2. Annual retraining and refresher for regular employees.
     - Develop a formal procedure document to incorporate risk identified in the environment into the security awareness education and update the awareness education material at least bi-annually.

- Management Support: Obtain support and commitment from top management to prioritize and allocate resources for security awareness training.
- Risk-based Approach: Based on risk assessment of the organization's specific security risks and tailor the training program to address those risks effectively. Focus on the most relevant and critical topics that align with the organization's industry, regulatory requirements, and potential threats.
- Training Objectives: Clearly define the objectives of the security awareness training program.
- Content Development: Develop engaging and interactive training materials that are relevant to the employees' roles and responsibilities.
- Training Delivery: Determine the most suitable delivery methods for the training, considering the organization's size, geographical distribution, and available resources.
- Frequency and Reinforcement: Establish a regular training schedule, considering the evolving nature of security threats.
- Measurement and Evaluation: Define metrics and evaluation mechanisms to assess the effectiveness of the training program.
- Compliance and Reporting: Ensure that security awareness training is aligned with relevant internal requirements and industry standards. Keep records of employee participation and completion of training activities to demonstrate compliance if required.
- Tailoring for Different Audiences: Recognize that different employee groups may have varying levels of technical expertise or job requirements. Tailor the training content and delivery methods to suit the needs of different departments, roles, and skill levels within the organization. Consider on-demand training to be published on the Learning Management System so that not only the current staff, but new staff can take advantage of it.

- Develop cyber incident management guideline.
  - Develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
  - Create and draft procedure document for reporting, escalation, investigation, and resolution process incidents which impact exposure of personal and sensitive information. SLA and metrics should be established to determined and measure effectiveness of the process.
  - Incident Response Plan: Develop a comprehensive incident response plan (IRP) that outlines the organization's strategy, goals, and processes for responding to cyber incidents.
  - Incident Classification and Escalation: Establish a clear incident classification framework that categorizes incidents based on their severity and impact. Define appropriate escalation paths for different types of incidents to ensure that the right individuals or teams are notified and involved in a timely manner.
  - Incident Response Team: Identify and train an incident response team (IRT) composed of individuals with the necessary technical expertise and authority to manage cybersecurity incidents.
  - Incident Detection and Reporting: Implement robust monitoring and detection mechanisms to identify and report potential cyber incidents promptly. This may involve the use of intrusion detection systems, security information and event management (SIEM) tools, log analysis, network monitoring, and threat intelligence feeds.
  - Communication and Stakeholder Engagement: Establish effective communication channels and protocols for reporting and sharing information about cyber incidents within the organization.
  - Incident Containment and Mitigation: Define processes and procedures for containing and mitigating cyber incidents to prevent further damage and minimize the impact on the organization.

- Forensic Investigation: Develop guidelines for conducting forensic investigations to determine the root cause of cyber incidents, identify the extent of the compromise, and collect evidence for potential legal actions or disciplinary measures.
- Business Continuity and Recovery: Establish strategies and plans for business continuity and recovery following a cyber incident. This includes defining procedures for system restoration, data recovery, backup management, and testing the effectiveness of incident response and recovery plans.
- Lessons Learned and Continuous Improvement: Conduct thorough post-incident analysis and documentation of lessons learned. Identify areas for improvement in the incident response processes, technical controls, training, or policy implementation. Incorporate these insights into future incident response planning and training activities.
- Testing and Exercises: Regularly conduct testing and simulation exercises to assess the effectiveness of the cyber incident management processes, validate the response capabilities, and identify areas for improvement.

- Define threat intelligence procedure.
  - Integrate the workflow of threat intelligence into security operations. This could include automating alerts based on specific indicators of compromise, adding threat intelligence data to incident reports, or prioritizing incidents based on threat severity.
  - Defined Objectives: Clearly define the objectives of the threat intelligence program. This includes identifying the specific goals, such as enhancing incident detection, improving incident response capabilities, identifying emerging threats, or supporting strategic decision-making.
  - Governance and Leadership: Assign clear ownership and responsibility for the threat intelligence program.
  - Information Sources: Establish a diverse range of information sources for collecting threat intelligence. This may include open-source intelligence (OSINT), commercial threat feeds, industry-specific information sharing and analysis centers (ISACs), government sources, vendor relationships, and internal data sources such as security logs and incident reports.
  - Threat Data Collection: Implement mechanisms for collecting and aggregating threat data from various sources.
  - Threat Analysis Capabilities: Develop robust capabilities for analysing and processing threat intelligence data.
  - Contextual Analysis: Conduct contextual analysis of threat intelligence data to understand its relevance and potential impact on the organization. This involves correlating threat information with the organization's assets, vulnerabilities, and existing security controls to assess the level of risk and prioritize response efforts.
  - Timeliness and Accuracy: Emphasize the importance of timeliness and accuracy in threat intelligence. Establish processes for validating and verifying threat data to ensure its reliability. Implement mechanisms for real-time or near-real-time intelligence updates to enable timely decision-making and response.
  - Intelligence Sharing and Collaboration: Foster a culture of intelligence sharing and collaboration both within the organization and with external partners.
  - Integration with Security Operations: Integrate threat intelligence into security operations processes and tools.
  - Training and Skills Development: Provide ongoing training and skills development opportunities for the threat intelligence team and other security personnel. Ensure that analysts are equipped with the necessary knowledge and tools to effectively utilize and interpret threat intelligence.

- Define of a Data Protection Guideline

- This guideline should clearly define the organization’s commitment in protecting and securing all data used, processed stored and managed within its environment.
- Developing a formalized, documented, and approved disposal policy or disposal of media which contains confidential information. Disposal policy should be aligned with legal requirements, value, criticality, and sensitivity. a. media containing confidential information should be stored and disposed of securely, e.g., by incineration or shredding, or erasure of data.
- Define roles and responsibilities of employee, contractors, and third-party provider to establish accountability in handling company, client, and personal data.
- Develop Cloud DLP governance procedures to protect corporate data being transmitted and stored on cloud apps.

- Developing data classification guideline
  - Outlines the process and criteria for classifying data based on its sensitivity, value, and the level of protection required. It helps the organization establish consistent and appropriate controls for handling different types of data.
  - Classification Categories: Define clear and specific data classification categories that align with the organization's needs and regulatory requirements. Each category should have a clear definition and criteria for inclusion.
  - Data Classification Criteria: Establish criteria for assigning data to different classification categories. Consider factors such as data sensitivity, potential impact of unauthorized disclosure or loss, regulatory requirements, contractual obligations, and business impact. Clearly define the attributes and characteristics that determine the classification level.
  - Ownership and Accountability: Define roles and responsibilities for data owners who are accountable for classifying and managing data within their areas of responsibility. Data owners should have a clear understanding of their roles and the importance of data classification for protecting sensitive information.
  - Data Handling Guidelines: Provide guidelines and specific requirements for each data classification category. Specify appropriate access controls, storage requirements, transmission mechanisms, encryption, disposal methods, and other security measures based on the sensitivity of the data. Consider legal and regulatory requirements when defining these guidelines.
  - Data Handling Procedures: Document procedures for handling data at each classification level. Specify how data should be accessed, stored, transmitted, and disposed of securely. Include guidelines for handling data in different formats, such as electronic files, physical documents, or cloud-based storage.
  - User Awareness and Training: Conduct regular training and awareness programs to educate employees about data classification, its importance, and their responsibilities. Ensure that employees understand how to identify, handle, and protect data based on its classification level. Train employees on the procedures and tools used for data handling.
  - Data Classification Tools and Technologies: Implement or identify appropriate tools and technologies that can assist in automating the data classification process. These tools can help identify sensitive data, enforce classification labels, and apply security controls consistently across the organization.
  - Review and Reclassification: Establish a regular review process to reassess the classification of data based on changes in its sensitivity or value. This includes periodic audits and updates to ensure that the classification remains accurate and relevant.
  - Incident Response and Reporting: Define procedures for responding to incidents involving classified data, including unauthorized access, loss, or disclosure. Specify reporting requirements, escalation paths, and the involvement of data owners and incident response teams in addressing and resolving such incidents.

- Monitoring and Enforcement: Implement mechanisms for monitoring and enforcing adherence to the data classification guideline. This includes regular audits, access controls, data loss prevention (DLP) technologies, and monitoring of user activities to detect and prevent unauthorized access or data handling violations.
- Documentation and Records: Maintain records of data classification decisions, classification changes, and related documentation. This documentation can serve as evidence of compliance, assist in incident investigations, and support accountability and audit requirements.

- Develop digital certificate and encryption key management procedure.
  - The procedure focuses on the use, protection and lifetime of encryption keys and certificates through the whole lifecycle, including generating, storing, archiving, retrieving, distributing, retiring, and destroying keys and certificates.
  - Certificate and key management outline the processes and controls necessary for managing digital certificates and encryption keys within an organization.
  - Inventory: Maintain an accurate and up-to-date inventory of all digital certificates used within the organization. This includes information such as certificate types, expiration dates, associated systems or services, and responsible personnel.
  - Lifecycle Management: Define the processes for digital certificate and encryption key lifecycle management, including issuance, renewal, revocation, and expiration.
  - Issuance and Registration: Establish controls for issuance and registration to ensure that only authorized individuals or systems can obtain and use digital certificates and encryption keys. Implement verification processes to validate the identity of certificate applicants and their authorization to request certificates.
  - Certificate Authority (CA) Management: Establish guidelines for managing the organization's relationship with certificate authorities. Define criteria for selecting trusted CAs and establish processes for obtaining and managing certificates from these authorities. Maintain records of CA certificates and ensure their validity.
  - Certificate Renewal and Expiration: Define procedures for monitoring and managing certificate expirations. Establish notification mechanisms to alert certificate owners in advance of certificate expirations to facilitate timely renewal or reissuance.
  - Certificate Revocation: Establish processes for certificate revocation in the event of compromise, key compromise, employee termination, or other security incidents. Ensure that certificate revocation lists (CRLs) or online certificate status protocol (OCSP) services are maintained and regularly updated to reflect revoked or expired certificates.
  - Certificate Storage and Protection: Implement secure storage mechanisms for digital certificates to prevent unauthorized access or disclosure. Consider using secure hardware modules or software-based key stores to protect private keys associated with the certificates.
  - Key Pair Generation and Management: Define procedures for secure key pair generation and management. Ensure that private keys are adequately protected and that key pairs are securely distributed to authorized certificate owners. Implement strong key management practices, including periodic key rotation or reissuance.
  - Certificate Auditing and Compliance: Implement mechanisms to track and monitor certificate usage and compliance with internal policies and industry standards. Conduct periodic audits of certificate management processes to ensure adherence to established procedures and detect any potential vulnerabilities or deviations.
  - Disaster Recovery and Backup: Establish procedures for backing up and recovering certificates in the event of system failures, disasters, or data loss. Implement appropriate redundancy and disaster recovery measures to ensure the availability and integrity of critical certificates.

- Documentation and Recordkeeping: Maintain comprehensive documentation of certificate management processes, including procedures, policies, audit records, and incident response plans. Document the roles and responsibilities of individuals involved in certificate management.

- Develop cloud service security management procedure.
  - The Cloud Service Security Management Procedure outlines the processes and controls required to manage the security of cloud services utilized by an organization. It ensures the protection of data, systems, and assets within the cloud environment.
  - Cloud Service Provider (CSP) Selection: Define criteria and requirements for selecting reliable and trustworthy cloud service providers. Consider factors such as security certifications, compliance with industry standards, data protection practices, incident response capabilities, and contractual obligations.
  - Service Level Agreements (SLAs): Establish clear and comprehensive SLAs with the cloud service provider to ensure that security requirements and expectations are met. Define performance metrics, security controls, incident response procedures, and responsibilities of both parties.
  - Risk Assessment and Due Diligence: Perform a comprehensive risk assessment of the cloud services and evaluate the associated risks. Conduct due diligence to assess the cloud service provider's security capabilities, infrastructure, data protection practices, and overall risk posture.
  - Data Classification and Encryption: Classify data based on its sensitivity and define encryption requirements for data at rest and in transit within the cloud environment. Implement encryption mechanisms and key management practices to protect data from unauthorized access or disclosure.
  - Identity and Access Management (IAM): Implement strong identity and access management controls within the cloud environment. Define access controls, role-based access policies, and authentication mechanisms to ensure that only authorized users can access resources and data within the cloud services.
  - Data Loss Prevention (DLP): Implement data loss prevention mechanisms to prevent the unauthorized disclosure or loss of sensitive data within the cloud environment. Define DLP policies, monitor data transfers, and implement controls to prevent data leakage.
  - Security Monitoring and Logging: Establish mechanisms to monitor the security of the cloud services and detect potential security incidents or vulnerabilities. Implement logging and auditing capabilities to track and analyse system activities, access events, and security-related events within the cloud environment.
  - Incident Response and Recovery: Define incident response procedures specific to cloud services. Establish communication channels, incident reporting mechanisms, and coordination with the cloud service provider in case of security incidents. Develop incident response and recovery plans tailored to the cloud environment.
  - Vulnerability Management: Implement a vulnerability management process to identify, assess, and mitigate vulnerabilities within the cloud services. Regularly scan and assess the security posture of the cloud infrastructure and applications and apply security patches and updates in a timely manner.
  - Business Continuity and Disaster Recovery: Define business continuity and disaster recovery procedures for the cloud environment. Establish backup and recovery mechanisms, data replication strategies, and disaster recovery testing processes to ensure the availability and resilience of critical cloud services.

- Develop security penetration test and remediation procedure.

- Information security penetration testing involves assessing the security of a system or network by simulating real-world attacks. The primary goal is to identify vulnerabilities that could be exploited by malicious actors and to provide recommendations for remediation.
- Scope Definition: Clearly define the scope of the penetration testing engagement, including the systems, networks, applications, or infrastructure components that will be tested. This helps establish the boundaries and objectives of the testing exercise.
- Rules of Engagement: Establish the rules of engagement to ensure all parties involved understand the limitations, testing methods, and constraints. This includes defining what types of attacks are allowed, specifying testing hours, and identifying any sensitive areas or critical systems that should be excluded.
- Testing Methodology: Select and follow an industry-standard penetration testing methodology, such as the Open Web Application Security Project (OWASP) Testing Guide or the Penetration Testing Execution Standard (PTES). These methodologies provide structured approaches for identifying and assessing vulnerabilities.
- Vulnerability Identification: Conduct various techniques and tests to identify vulnerabilities, including network scanning, vulnerability scanning, manual security testing, social engineering, and exploitation attempts. This involves using both automated tools and manual techniques to discover weaknesses and potential points of entry.
- Vulnerability Analysis: Analyse the vulnerabilities identified during the testing phase to determine their severity, impact, and potential exploitability. This helps prioritize remediation efforts based on the risk they pose to the system or network.
- Report Generation: Prepare a comprehensive report that includes a detailed analysis of the vulnerabilities discovered, their potential impact, and recommendations for remediation. The report should be clear, concise, and actionable, providing specific steps and guidance to address each identified vulnerability.
- Remediation Planning: Develop a remediation plan based on the findings of the penetration test report. This plan should prioritize the vulnerabilities based on their risk level and provide clear instructions for fixing or mitigating each vulnerability.
- Remediation Implementation: Execute the remediation plan by addressing the identified vulnerabilities, applying necessary patches and updates, configuring security settings, or implementing additional security measures as recommended.
- Retesting: After remediation, conduct a retest or follow-up penetration testing to verify that the identified vulnerabilities have been effectively addressed. This helps ensure that the security measures implemented are working as intended and that new vulnerabilities have not been introduced inadvertently.
- Continuous Improvement: Establish a process for ongoing monitoring, assessment, and improvement of the system's security posture. Regularly review and update security measures, perform periodic penetration testing, and stay informed about emerging threats and vulnerabilities.

- Develop a KPI standard for information security.
    - Key Performance Indicators (KPIs) for information security help measure the effectiveness, efficiency, and performance of an organization's security program. While specific KPIs may vary depending on the organization's goals, industry, and security objectives, here are some typical KPIs for information security:
    - Number of Security Incidents: Measure the number of security incidents reported over a specific period to assess the overall security incident trend and identify potential areas of concern.

- Mean Time to Detect (MTTD): Calculate the average time it takes to detect security incidents from the moment they occur. A lower MTTD indicates faster detection and a more proactive security posture.
- Mean Time to Respond (MTTR): Determine the average time it takes to respond to and resolve security incidents. A lower MTTR indicates a more efficient incident response process.
- Percentage of Security Awareness Training Completion: Track the percentage of employees who have completed security awareness training. This helps assess the level of security awareness and knowledge within the organization.
- Compliance with Security Policies: Monitor the organization's adherence to security policies and controls, ensuring compliance with regulatory requirements and internal security standards.
- Patch Management Effectiveness: Measure the timeliness and completeness of patch management activities to assess the organization's ability to mitigate vulnerabilities and protect against known security flaws.
- Number of Vulnerabilities Identified and Remediated: Track the number of vulnerabilities identified through assessments and vulnerability scans, as well as the number of vulnerabilities successfully remediated.
- Security Audit Findings and Remediation Rate: Monitor the number and severity of security audit findings and track the rate at which they are addressed and resolved.
- Percentage of Critical Systems with Up-to-Date Security Controls: Assess the percentage of critical systems that have up-to-date security controls in place, such as firewalls, intrusion detection systems, and access controls.
- Employee Security Training Feedback: Collect feedback from employees on the quality and effectiveness of security training programs to gauge their perception of the training's value.
- Phishing Click Rate: Measure the percentage of employees who fall victim to phishing attacks, helping identify potential weaknesses in security awareness and training.

4. Information and Cyber Security Policy, Process and Governance Documents to be reviewed and updated.

- **Review and update Information Security Policy**
  - Information Security Policies serve as a foundation for an organization's security program and provide guidance on the principles, expectations, and requirements for protecting information assets. It is a vital part of the organization's technology policies.
  - Assist in developing a plan to ensure the information security strategy is established, implemented, documented, and communicated with clearly defined mission and vision statements throughout the organization.
  - Develop a formal cybersecurity relationship management framework and operating model, including the documented roles responsible for working with IT and business stakeholders.
  - Assist in developing a cybersecurity future state roadmap and engage executive leadership to review the roadmap annually.
  - Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations.
  - Establish policies and procedures based on industry related frameworks. (NIST, ISO, FFIEC, FSSCC HIPAA, HITRUST, etc.)
  - Draft a clear guideline on how cyber risk information are to be communicated among employees, contractors, and third-party provider. Employees, third-party contractors are aware of their roles and responsibilities with regards to cyber security risks.

- Policy Scope and Applicability: Clearly define the scope of the policy and identify the systems, data, and personnel to which it applies. Specify whether the policy covers employees, contractors, third-party vendors, or any other relevant stakeholders.
- Information Security Objectives: Clearly state the objectives of the information security program and align them with the organization's overall business goals. This helps ensure that security measures are implemented to support the organization's mission and protect its critical assets.
- Roles and Responsibilities: Define the roles and responsibilities of individuals involved in information security, including management, system administrators, data owners, and users. Clarify their obligations in protecting information assets and enforcing security controls.
- Risk Management: Include provisions for risk assessment, risk treatment, and ongoing risk management activities. This involves identifying and assessing information security risks, implementing appropriate controls, and monitoring the effectiveness of those controls.
- Asset Classification and Protection: Establish guidelines for the classification of information assets based on their sensitivity and criticality. Specify how assets should be protected, including access controls, encryption requirements, and data handling procedures.
- Access Control: Define the principles and practices for granting, modifying, and revoking access rights to information resources. Include guidelines for user authentication, password management, least privilege, and separation of duties.
- Incident Response and Reporting: Establish procedures for detecting, reporting, and responding to security incidents. Define the roles and responsibilities of incident response teams, incident reporting mechanisms, and escalation procedures.
- Security Awareness and Training: Outline the requirements for security awareness programs and training initiatives. Specify the frequency and topics of security training, as well as the responsibilities of employees to participate and adhere to security policies.
- Physical Security: Include provisions for physical security controls to protect information assets. Define guidelines for access control to physical premises, secure disposal of sensitive materials, and protection of equipment and media.
- Third-Party Security: Address the security requirements for engaging with third-party vendors, contractors, and business partners. Specify the expectations for their handling of sensitive information and their adherence to security controls.
- Compliance and Legal Requirements: Ensure that the policy addresses relevant legal, regulatory, and contractual obligations. Specify how the organization will monitor compliance, report incidents, and handle breaches to comply with applicable laws and regulations.
- Policy Review and Maintenance: Establish a process for reviewing, updating, and communicating the policy on a regular basis. Assign responsibility for policy maintenance and ensure that the policy remains aligned with changing business needs, technology advancements, and evolving security threats.

- Review and update data leakage prevention guideline
  - Integrate with a data classification framework that categorizes data based on its sensitivity, criticality, and regulatory requirements. Clearly define the application of classification levels and labelling mechanisms to enable accurate identification and protection of sensitive data.
  - Data Discovery and Inventory: Establish procedures and tools to identify, discover, and maintain an inventory of sensitive data within the organization. Regularly scan systems,

databases, file shares, and other repositories to identify the presence and location of sensitive data.

- Data Handling Policies and Procedures: Develop clear policies and procedures for handling sensitive data throughout its lifecycle. Define guidelines for data collection, storage, transmission, access, sharing, and disposal to ensure proper data protection at all stages.
- Access Controls and User Authentication: Implement strong access controls and user authentication mechanisms to ensure that only authorized individuals can access and handle sensitive data. Use techniques such as role-based access control (RBAC), two-factor authentication (2FA), and strong password policies.
- Encryption and Data Protection: Implement encryption mechanisms, both at rest and in transit, to protect sensitive data from unauthorized access or disclosure. Define encryption requirements based on the data classification levels and industry best practices.
- Network and Perimeter Security: Establish network security measures, such as firewalls, intrusion detection/prevention systems (IDS/IPS), and secure gateways, to monitor and control data flows across the network perimeter. Implement network segmentation and traffic monitoring to prevent unauthorized data exfiltration.
- Data Loss Prevention Tools: Deploy Data Loss Prevention (DLP) tools or solutions that enable real-time monitoring and detection of sensitive data leakage attempts. Configure the DLP system to identify and block data leakage through various channels, such as email, web uploads, removable media, or cloud storage.

- Review and update Privileged access management procedure.
  - The Privileged Access Management (PAM) procedure should consider the following requirements to effectively manage and control privileged access:
  - Privileged Account Identification and Inventory: Identify all privileged accounts within the organization's systems, applications, and network infrastructure. Maintain an inventory of these accounts, including details such as account names, owners, and associated privileges.
  - Privileged Account Management Lifecycle: Define processes for managing privileged accounts throughout their lifecycle, including provisioning, deprovisioning, and periodic review of privileges. Implement mechanisms to ensure that privileged accounts are only granted to authorized individuals and are revoked promptly when no longer needed.
  - Role-Based Access Control: Implement a role-based access control (RBAC) model for privileged accounts. Define roles and associated privileges based on job functions and responsibilities. Grant privileges to individuals based on their roles, reducing the number of directly assigned privileged accounts.
  - Just-in-Time Privileged Access: Implement just-in-time (JIT) access controls for privileged accounts. Grant temporary and time-limited access to privileged accounts based on the specific tasks or activities that require elevated privileges. Monitor and log all activities during JIT access.
  - Multi-Factor Authentication (MFA): Implement multi-factor authentication for privileged accounts to ensure stronger authentication and mitigate the risk of unauthorized access. Require at least two factors for authentication, such as a password, a smart card, a biometric factor, or a token.
  - Privileged Session Monitoring: Implement session monitoring and recording capabilities for privileged accounts. Monitor and log all activities performed during privileged sessions to detect any suspicious or unauthorized actions. Review session logs regularly for auditing and investigation purposes.
  - Least Privilege Principle: Apply the principle of least privilege to privileged accounts. Grant the minimum level of privileges necessary for individuals to perform their job functions. Regularly review and remove unnecessary privileges from privileged accounts.

- Password Management: Implement strong password management practices for privileged accounts. Enforce password complexity requirements, regular password rotation, and password vaulting solutions to securely store and manage privileged account credentials.
- Segregation of Duties: Implement segregation of duties (SoD) controls to prevent conflicts of interest and reduce the risk of unauthorized actions. Ensure that no single individual has excessive privileges or controls over critical systems or processes.
- Privileged Access Request and Approval: Establish a formal process for requesting and approving privileged access. Define guidelines for submitting access requests, obtaining appropriate approvals, and documenting the purpose and duration of privileged access.
- Regular Auditing and Review: Conduct regular audits and reviews of privileged accounts, their usage, and associated privileges. Ensure compliance with policies, identify any unauthorized activities, and address any deviations from established controls promptly.
- Training and Awareness: Provide comprehensive training and awareness programs to individuals with privileged access. Educate them on their responsibilities, the risks associated with privileged access, and the importance of adhering to PAM procedures.

- Review and update Vulnerability management guideline
  - Vulnerability Scanning: define and implement a vulnerability scanning solution to regularly scan the organization's systems, applications, and network infrastructure for known vulnerabilities. Choose a reputable scanning tool that provides comprehensive coverage and accuracy.
  - Asset Inventory: Maintain an up-to-date inventory of all systems, applications, and network devices within the organization. This inventory should include information such as system owners, criticality, and contact details.
  - Vulnerability Assessment Frequency: Define the frequency of vulnerability assessments based on the organization's risk profile, the criticality of assets, and industry best practices. Regularly scheduled scans should be conducted, along with additional scans triggered by significant changes to the environment.
  - Patch Management Process: Establish a patch management process to promptly identify, test, and deploy patches for known vulnerabilities. Define responsibilities, timelines, and procedures for patching systems and applications, ensuring critical patches are prioritized.
  - Vulnerability Remediation Prioritization: Develop a risk-based approach to prioritize vulnerability remediation efforts. Consider the severity of the vulnerability, the potential impact on the organization, and the likelihood of exploitation when determining the order of remediation.
  - Vulnerability Tracking and Monitoring: Implement a system for tracking and monitoring vulnerabilities throughout their lifecycle. Maintain an inventory of vulnerabilities, including their status, remediation plans, and assigned owners. Regularly review and update vulnerability information as remediation efforts progress.
  - Vulnerability Reporting and Communication: Establish a process for reporting vulnerabilities to relevant stakeholders, including system owners, IT teams, and management. Develop clear and concise vulnerability reports that provide actionable information for remediation efforts.
  - Vulnerability Remediation Validation: Verify the effectiveness of vulnerability remediation efforts through post-remediation scans or penetration testing. Validate that vulnerabilities have been properly mitigated and that new vulnerabilities have not been introduced during the remediation process.
  - Vulnerability Disclosure and Coordination: Define procedures for responsible vulnerability disclosure and coordination with external entities, such as software vendors or security

researchers. Establish communication channels and processes for reporting vulnerabilities and tracking their resolution.

- Review and update Information security operation center operation procedure
    - SOC Scope and Responsibilities: Clearly define the scope of the SOC's operations and its responsibilities within the organization. Specify the types of security incidents and events that the SOC is responsible for monitoring, detecting, analysing, and responding to.
    - Incident Handling Process: Establish an incident handling process that outlines the steps and procedures for handling security incidents. Define roles and responsibilities, escalation paths, and communication channels for incident response within the SOC.
    - Security Monitoring and Event Management: Implement security monitoring tools, such as Security Information and Event Management (SIEM) systems, log management solutions, and intrusion detection systems (IDS). Define processes for collecting, analysing, and correlating security events to identify potential security incidents.
    - Threat Intelligence Integration: Incorporate threat intelligence feeds into the SOC's operations. Establish processes for consuming and analysing threat intelligence information to proactively identify emerging threats and enhance the organization's defences.
    - Alert Management and Triage: Define procedures for managing security alerts generated by monitoring systems. Establish criteria for alert prioritization, classification, and triage based on their severity, impact, and likelihood. Develop playbooks and response guidelines for different types of alerts.
    - Incident Response Coordination: Establish processes for coordinating incident response efforts within the SOC. Define communication channels, incident coordination mechanisms, and integration with other teams or departments involved in incident response, such as IT, network, or legal teams.
    - Reporting and Metrics: Establish reporting mechanisms to provide regular updates on the SOC's activities, incident trends, and performance metrics. Define key performance indicators (KPIs) to measure the effectiveness and efficiency of the SOC's operations.
    - Incident Analysis and Forensics: Define processes for analysing and investigating security incidents. Establish procedures for collecting and preserving evidence, conducting root cause analysis, and performing forensic investigations when required.
    - Change Management: Develop change management processes specific to the SOC's operations. Establish guidelines for implementing changes to security monitoring systems, detection rules, or incident response processes to ensure proper testing, approval, and documentation.
    - Knowledge Management: Establish procedures for documenting and sharing knowledge within the SOC. Develop a knowledge base or repository that captures incident response playbooks, incident handling procedures, and lessons learned to facilitate continuous improvement.
    - Continuous Improvement and Quality Assurance: Regularly review and assess the SOC's operations to identify areas for improvement. Conduct periodic audits or assessments to evaluate the effectiveness of processes, tools, and personnel performance. Incorporate lessons learned and feedback to enhance the SOC's capabilities.

- Review and update IT system baseline and hardening standard
    - A system baseline and hardening standard provide guidelines for establishing secure and consistent configurations for computer systems, networks, infrastructure components, integration, and security systems within the organization.

- Asset Inventory: Maintain an up-to-date inventory of all systems and infrastructure components within the organization. This includes servers, workstations, network devices, databases, and other relevant assets.
- Configuration Management: Implement a configuration management process to establish and maintain secure baselines for each system or component. Define standard configurations that align with industry best practices, vendor recommendations, and security requirements.
- Secure Configuration: Develop detailed guidelines for secure configuration settings, considering factors such as operating system versions, software applications, network devices, and hardware platforms. Specify secure settings for system parameters, services, user accounts, access controls, encryption, logging, and auditing.
- Least Privilege: Implement the principle of least privilege by granting users the minimum privileges necessary to perform their tasks. Define user roles, permissions, and access rights based on job requirements. Regularly review and update user privileges as roles change.
- Password and Authentication Policies: Establish password and authentication policies that enforce strong passwords, password expiration, account lockout, and multi-factor authentication (MFA) where appropriate. Specify requirements for password complexity, length, and uniqueness.
- Network Security: Define guidelines for securing network configurations, including firewall rules, intrusion prevention systems (IPS), virtual private networks (VPNs), wireless networks, and remote access. Implement secure network segmentation to limit unauthorized access and lateral movement within the network.
- Encryption: Specify encryption requirements for data in transit and at rest, depending on the sensitivity of the information and applicable regulatory requirements. Define encryption algorithms, key management practices, and use of digital certificates for secure communication.
- Logging and Auditing: Establish guidelines for logging and auditing activities to ensure visibility into system events and potential security incidents. Define log retention periods, event types to be logged, and requirements for log analysis and review.
- System Monitoring and Incident Response: Define requirements for system monitoring and incident response. Implement mechanisms to detect and alert on suspicious activities, unauthorized access attempts, or security breaches. Establish procedures for incident response, including reporting, investigation, containment, and recovery.

Non-Functional Requirements

Non-functional requirements define the technical standards and quality attributes of the system, for instance, system usability, effectiveness, security, scalability, etc.

1. Service resource should mainly work with NDB HQ staff.
2. English is mandatory as the medium of communication and documentation.

NDB Information Technology
Guideline and Procedure Consultancy Service
Requirements Specification

Version 1.0
2023.07.24

Executive Summary

Project Description

This project is to request information technology process and governance consultancy service to:

4. Review and develop the required policies, guidelines and procedures in accordance with industry best-practices frameworks and the business reality of NDB.
5. Recommendations of architecting and implementing these processes and policies organizationally and systematically.
6. Review and recommend other necessary process definitions which are not covered in the current governing system and the requirement in this document.

Functions and Features

Functional Requirements

Functional requirements define the features the service must provide.

FR1.	General requirement to the consulting team

- Expertise and Experience: The consulting team should have a strong background and extensive experience in IT management and governance. They should possess deep knowledge of industry best practices, frameworks (such as ITIL, COBIT), and regulatory requirements related to IT management and governance, especially the financial industry and MDB (multilateral development bank) community.

- Relevant Skills and Certifications: The consulting team should have a team of consultants with the necessary skills and certifications. This may include certifications such as ITIL Foundation, COBIT, PMP (Project Management Professional), or CISA (Certified Information Systems Auditor). Ensure that the team has expertise in areas such as IT strategy, IT service management, IT governance, risk management, and compliance.

- Understanding of Organizational Context: The consulting team should demonstrate a strong understanding of NDB's organization, industry, size, complexity, and specific IT management and governance challenges. They should be able to align the recommendations and solutions with NDB's context and strategic objectives.

- Methodology and Approach: The consulting team should have a structured and proven approach for conducting assessments, developing policies and frameworks, and implementing governance structures. This ensures a systematic and effective engagement.

- Collaboration and Communication: The consulting team should demonstrate excellent communication skills, actively listen to NDB's needs and requirements, and foster collaborative working relationships with project stakeholders.

- Tailored Solutions: Look for a consulting team that can provide tailored solutions to meet your specific needs. They should be able to customize policies, frameworks, and governance structures to align with NDB's culture, processes, and industry regulations.

- Project Management and Timelines: The consulting team should have a track record of delivering projects on time and within budget, proven project management methodologies, deliverable milestones, and reporting mechanisms to ensure effective project oversight and transparency.

- References and Reputation: The consulting team should have high reputation in the industry with testimonials, case studies, or client success stories that demonstrate their ability to deliver value and achieve desired outcomes.

- The consultant team should support the clarification and necessary revision of the defined and revised policies, guidelines, and procedures through NDB internal review and approval.

FR2. General requirement to the policies, guidelines, and procedures to be developed or updated.

- Establish policies and procedures based on industry related frameworks (ITIL, COBIT, CMMI, ISO38500, etc) and cross match to ensure the completeness of principles of the frameworks adaptable to NDB are in place.
- Review, update and streamline IT policy document hierarchy.
- Guideline document has its direct impact and requirement to IT and other business units, which Procedure document are mainly for IT internally.
- Foster a culture of continuous improvement of the related process. Regularly review and evaluate the effectiveness of the process, seek feedback from stakeholders, and implement improvements to enhance efficiency, minimize risk, and improve overall service delivery management and quality.
- Compliance and Reporting: Ensure that the policy, guideline, and procedures comply with applicable industry and internal regulation and requirements.
- Provide training and awareness programs to relevant stakeholders, including IT staff and end users, to educate them about the related process, roles and responsibilities, and the importance of reporting promptly and accurately. This helps ensure consistent understanding and adherence to the regulatory document.
- Define metrics and key performance indicators (KPIs) to measure the effectiveness and value of the defined guidelines and procedures.

FR3. Information Technology Process and Governance Documents to be developed.

- **Develop a service provider management guideline.**
    - Define criteria, processes, and procedures for selecting technology solution vendors and monitoring the vendor's adherence to established information technology and security requirements.

- Service scope: Clearly define the category and range of services offered by the IT service provider, including areas of expertise, technology platforms, geographic locations, specific solutions, and other necessary factors related to supplier and contract management.

- Service Level Agreements (SLAs): Establish measurable performance targets and metrics for service delivery, such as response time, uptime, and resolution time. SLAs should align with business requirement and ensure consistent service quality.

- Security and Data Protection: Define security protocols, data protection measures, and confidentiality practices to safeguard NDB data and IT systems. This may include encryption, access controls, incident response procedures, and compliance with relevant regulations.

- Customer Support: Outline the support channels available to NDB, such as a call centre, customer success manager, help desk, ticketing system, or knowledge base. Specify response times, escalation procedures, and the availability of technical support staff.

- Change Management: Establish procedures for managing changes to IT systems, including documentation, testing, and communication protocols. This ensures that changes are implemented smoothly and minimize disruptions.

- Disaster Recovery and Business Continuity: Define strategies and processes to recover from IT system failures, natural disasters, or other emergencies. This includes backup procedures, RPO, RTO, disaster recovery plans, and periodic testing to ensure data integrity and minimize downtime.

- Performance Monitoring and Reporting: Specify mechanisms for monitoring IT system performance, collecting relevant data, and generating reports.

- Service Assessment: Align with other concerned internal documentations, specify the criteria and procedure for supplier assessment before renewal or termination decisions.

- Training and Knowledge Management: Address the training needs from the IT service provider.

- **Develop an asset management guideline.**

  - Inventory Management: Maintain a comprehensive and up-to-date inventory of all IT assets, including hardware, software, and associated components.

  - Asset Classification: Classify assets based on their type, ownership, criticality, and lifecycle stage.

- Documentation: Create and maintain accurate documentation for each asset, including details such as asset description, specifications, purchase date, warranty information, and location.

- Asset Tracking: Track the movement and location of assets throughout their lifecycle. This ensures better visibility and control over asset utilization.

- Asset Lifecycle Management: Define and follow a standardized process for asset acquisition, deployment, maintenance, and retirement. This includes procedures for asset procurement, configuration, installation, and disposal.

- License Management: Monitor and manage licenses and subscriptions to ensure compliance with legal and contractual obligations. This involves tracking license and subscription usage, conducting regular audits, and managing software and other eligible entitlements.

- Change Management: Establish change control procedures to track and manage changes to IT assets, including software updates, hardware upgrades, and configuration modifications. This helps prevent unauthorized or unmanaged changes that could impact asset performance or security.

- Asset Security: Implement security measures to protect IT assets from unauthorized access, theft, or damage. This includes physical security controls, access controls, encryption, and vulnerability management.

- Asset Performance and Health Monitoring: Monitor the performance and health of IT assets to identify potential issues or vulnerabilities. Implement proactive maintenance and monitoring processes to ensure optimal asset performance.

- Reporting and Compliance: Generate regular reports on asset inventory, usage, and performance. Ensure compliance with relevant regulatory requirements and internal policies.

- Asset Disposal and Data Destruction: Define processes for the proper disposal of retired assets and the secure destruction of sensitive data. Comply with legal and environmental regulations for asset disposal.

- **Develop a software development management procedure.**

  - Requirement Gathering and Analysis: Clearly define the process for gathering, analysing, and validating user requirements. This includes techniques such as interviews, workshops, and documentation review to ensure a comprehensive understanding of user needs and alignment between stakeholders.

  - Design and Architecture: Specify the design of the software architecture based on industry-standard design patterns and architectural principles and tailored to the business

reality of the organization to ensure scalability, maintainability, and flexibility of the software., including the overall system structure, modules, and components. This involves creating design documents, diagrams, and prototypes to guide the development process.

- Coding Standards and Practices: Establish coding standards and best practices to ensure consistency, maintainability, and quality of the code.

- Version Control and Configuration Management: Implement version control practices and tools to manage source code changes, track revisions, and enable collaboration among developers. This helps maintain code integrity and facilitates rollbacks if necessary. Additionally, establish configuration management procedures to manage software configurations and dependencies.

- Testing and Quality Assurance: Define comprehensive test strategies the procedures for conducting various levels of testing, including unit testing, integration testing, system testing, and acceptance testing. This includes specifying the use of testing frameworks, tools, and techniques. Implement quality assurance practices to ensure the software meets specified requirements and quality standards.

- Change Management: Aligned other related internal documents in the areas of IT change management and project management, establish a change management process for managing changes to the software throughout its lifecycle. This includes documenting and assessing change requests, conducting impact analysis, and obtaining proper approvals. It helps control scope definition and ensures that changes are properly assessed and implemented.

- Documentation: Require comprehensive documentation and template where applicable throughout the development process, including software requirements, design specifications, user manuals, and release notes. This documentation aids in software maintenance, troubleshooting, and future enhancements.

- Deployment and Release Management: Define the procedures for deploying and releasing the software. This includes configuration management, deployment automation, versioning, and release notes. It ensures a controlled and smooth transition of the software from the development environment to the production environment.

- Security and Privacy: Incorporate security and privacy considerations and utilize appropriate tools into the software development procedure to ensure effeteness and security. This includes adhering to secure coding practices, conducting security reviews, implementing access controls, and ensuring data protection.

- User Training and Support: Specify the procedures for providing user training and ongoing support for the software. This includes creating user guides, providing training sessions, and establishing a support mechanism to handle user-reported issues.

- Maintenance and Enhancement: Aligning with related internal IT management documents, define the process for ongoing software maintenance, bug fixing, and enhancement. This includes tracking and prioritizing software issues, implementing change requests, and managing software updates and patches.

- Compliance and Legal Considerations: Ensure that the software development procedure complies with relevant legal and regulatory requirements, such as intellectual property rights, data protection regulations, and software licensing.

- **Develop a service configuration management procedure.**

  - Configuration Identification: Define a process for identifying and naming configuration items (CIs) within the service. This includes establishing a naming convention and maintaining a configuration management database (CMDB) or repository to store and manage CI information.

  - Configuration Baselines: Establish procedures for creating and maintaining configuration baselines for different versions or releases of the service. This ensures that a reference point is available for configuration changes and allows for effective change control.

  - Configuration Control: Define a change control process to manage configuration changes. This includes documenting and assessing change requests, conducting impact analysis, obtaining proper approvals, and maintaining a configuration change log.

  - Configuration Item Status Accounting: Implement mechanisms to track and report on the status and history of CIs. This involves maintaining accurate records of CI attributes, such as version, location, ownership, and relationships with other CIs.

  - Configuration Verification and Audit: Establish procedures for verifying the accuracy and completeness of configuration information. Conduct periodic configuration audits to ensure that the actual configurations align with the documented configurations.

  - Configuration Documentation: Require comprehensive documentation of configuration items, including specifications, dependencies, relationships, and configurations. This documentation should be up-to-date, easily accessible, and well-maintained.

  - Configuration Item Versioning: Implement version control practices for configuration items, especially for software or firmware components. This ensures that different versions or releases can be identified and managed appropriately.

  - Configuration Item Change Tracking: Track and document all changes made to configuration items, including the reason for the change, the person responsible, and the date of the change. This helps in tracing the history and impact of configuration changes.

- Configuration Item (Resource) Request and Approval: Establish a procedure for requesting and approving technology resources. This may involve standardized request forms, approval workflows, and defined criteria for resource allocation.

- Configuration Release and Deployment: Define procedures for the release and deployment of configuration items, including planning, testing, and coordination with other teams or stakeholders. This ensures controlled and consistent deployment of configurations across environments.

- Configuration Management Tools: Identify and utilize appropriate tools or software solutions to facilitate configuration management activities. These tools can assist in maintaining the CMDB, tracking changes, and generating reports.

- Configuration Reporting: Establish reporting mechanisms to communicate the status, performance, and compliance of configuration items. This includes generating reports on configuration baselines, changes, audits, and compliance with configuration management policies.

- Configuration Management and Service Lifecycle: Integrate the configuration management process with the overall service lifecycle management. Ensure that configuration management activities align with other IT service management processes, such as incident management, change management, and release management.

- **Develop a Network Operation Center (NOC) operation procedure.**

  - Roles and Responsibilities: Define the roles and responsibilities of NOC personnel, including operators, technicians, and managers. Clearly outline their duties, authority levels, and communication protocols to ensure effective coordination and accountability.

  - Incident Management: Aligning with related internal IT management documents about Incident Management and Service Monitoring and Log Management Procedure, establish procedures for the identification, logging, prioritization, and resolution of network incidents. This includes defining incident response times, escalation paths, and communication protocols for different severity levels of incidents.

  - Monitoring and Alerting: Implement network monitoring tools and define processes for real-time monitoring of network devices, links, and services. Configure alerts and notifications to proactively identify and respond to network issues or performance degradation.

  - Incident Response and Escalation: Aligning with related internal IT management document about Incident Management, define clear incident response procedures, including initial triage, troubleshooting steps, and escalation protocols. Establish a hierarchy of escalation contacts, both within the NOC team and with other IT teams or external vendors, to ensure timely incident resolution.

- Documentation and Reporting: Define the template for comprehensive documentation of incident reports, troubleshooting steps, and resolution procedures. Define the process and template for the generation of regular reports on network performance, incident trends, and key metrics to facilitate analysis and decision-making.

- Performance Monitoring and Capacity Planning: Define procedures for monitoring and managing network performance, including bandwidth utilization, latency, packet loss, and other key performance indicators (KPIs). Define the process to set performance thresholds, conduct capacity planning, and implement proactive measures to optimize network performance.

- Security Management: Aligning with related internal IT management document about Security Operation Procedure, incorporate security practices into NOC procedures, including monitoring for security events, applying security patches and updates, and enforcing access controls and authentication mechanisms. Ensure compliance with security standards and regulations.

- Communication and Collaboration: Define the process to establish communication and collaboration channels within the NOC team and with other stakeholders, such as IT teams, vendors, and customers. Define communication protocols, tools, and escalation procedures to ensure effective information exchange and timely updates.

- Training and Knowledge Management: Define the frequency and scope of ongoing training and knowledge sharing sessions to NOC staff to ensure they are equipped with the necessary skills and expertise. Define the process to develop and maintain a knowledge base or documentation repository to capture best practices, troubleshooting guides, and lessons learned.

- Continuous Improvement: Foster a culture of continuous improvement within the NOC by regularly reviewing and analysing performance metrics, incident trends, and customer feedback. Use this information to identify areas for improvement, implement process enhancements, and drive operational efficiency.

- **Develop a System and Application Integrated Operation Centre Procedure (IOC)**

  - Roles and Responsibilities: Define the roles and responsibilities of IOC personnel, including operators, technicians, and managers. Clearly outline their duties, authority levels, and communication protocols to ensure effective coordination and accountability.
  -
  - Centralized Monitoring and Control: The integrated operation centre should provide a centralized platform for monitoring and controlling various systems and processes within the organization. This includes monitoring infrastructure, applications, networks, security systems, and other critical components.

- Real-time Data and Analytics: The centre should have the capability to collect, analyse, and visualize real-time data from different sources. This enables effective monitoring, decision-making, and proactive response to incidents or events.

- Incident and Event Management: The integrated operation centre should have robust incident and event management capabilities. This includes the ability to receive, track, and manage incidents or events, assign ownership and responsibilities, and escalate issues as necessary.

- Collaboration and Communication: The centre should provide collaboration and communication tools to facilitate effective communication and coordination among different teams and stakeholders. This includes features such as chat, video conferencing, document sharing, and task management.

- Automation and Orchestration: Automation capabilities should be integrated into the operation centre to streamline routine tasks and processes. This can include automated incident triaging, event correlation, remediation workflows, and task automation to improve efficiency and response times.

- Integration with IT Service Management (ITSM): The operation centre should be tightly integrated with the IT service management processes and tools. This ensures seamless incident, problem, and change management, as well as accurate reporting and tracking of service-level agreements (SLAs).

- Visualization and Dashboards: The centre should provide customizable dashboards and visualization tools to present real-time data, key performance indicators (KPIs), and metrics in a clear and intuitive manner. This enables quick decision-making and provides situational awareness to stakeholders.

- Business Continuity and Disaster Recovery: The integrated operation centre should be capable of monitoring and managing business continuity and disaster recovery processes. This includes monitoring backup and recovery systems, conducting drills and exercises, and tracking the status of recovery plans.

- Security Monitoring and Threat Intelligence: this is covered in the Security Operation Center procedure.

- Scalability and Resilience: The operation centre should be designed to handle scalability and provide resilience. It should be able to accommodate growing volumes of data, monitor a wide range of systems and processes, and handle high availability requirements.

- Training and Skill Development: The centre should provide training and skill development programs for the staff involved in operations. This ensures that they have the necessary knowledge and expertise to effectively monitor, analyse, and respond to incidents and events.

- Continuous Improvement: The operation centre should foster a culture of continuous improvement. This includes regularly reviewing and refining processes, leveraging feedback and insights from operations, and incorporating lessons learned to enhance the centre's capabilities and effectiveness over time.

- **Develop a service monitoring and log management procedure.**

  - Monitoring Objectives: Define the objectives of system monitoring, such as identifying performance bottlenecks, detecting security incidents, or ensuring system availability. Establish specific metrics and thresholds to monitor for each objective.

  - Monitoring Tools and Technologies: Identify and implement appropriate monitoring tools and technologies to collect and analyse system metrics, health, availability, performance, and logs. This may include network monitoring tools, server monitoring agents, log management systems, or SIEM (Security Information and Event Management) solutions.

  - Monitoring Targets: Specify the systems, applications, and network components that need to be monitored. This includes servers, network devices, databases, applications, cloud services, and any other critical components of the system infrastructure.

  - Performance Monitoring: Define the parameters and metrics to be monitored for system performance, such as CPU utilization, memory usage, disk space, network bandwidth, response time, and application-specific metrics. Set thresholds for acceptable performance levels and configure alerts for deviations.

  - Security Monitoring: Establish procedures to monitor for security incidents, such as unauthorized access attempts, malware infections, or suspicious network traffic. Define the procedure to configure intrusion detection systems, log analysis tools, and other security monitoring mechanisms.

  - Log Collection and Centralization: Define the process for collecting and centralizing logs from various systems and applications. This may involve setting up log collectors, agents, or forwarding mechanisms to aggregate logs into a centralized log management system.

  - Log Retention and Storage: Determine the appropriate log retention period based on regulatory requirements, security needs, and operational considerations. Define procedures for archiving and storing logs securely, ensuring they are readily accessible for analysis and investigation.

  - Log Analysis and Alerting: Establish procedures for analysing logs to identify patterns, anomalies, and potential issues. Configure alerting mechanisms to notify appropriate personnel when specific log events or patterns occur, indicating a potential problem or security incident.

- Incident Response and Escalation: Define processes for incident response and escalation based on the severity of events detected through monitoring and log analysis. Establish communication channels, roles, and responsibilities to ensure timely and appropriate response to incidents.

- Regular Monitoring Reviews: Conduct regular reviews and analysis of monitoring data, performance metrics, and log analysis reports. Identify trends, patterns, and areas for improvement. Use this information to optimize system performance, enhance security measures, and fine-tune monitoring configurations.

- Compliance and Audit: Ensure that monitoring and log management procedures align with relevant compliance requirements, industry standards, and regulatory guidelines. Document procedures and maintain audit trails to demonstrate compliance during audits or investigations.

- Documentation and Reporting: Require comprehensive documentation of monitoring configurations, log management procedures, and incident response plans. Generate regular reports on system performance, security incidents, and compliance status. Use these reports for performance tracking, troubleshooting, and compliance monitoring.

- These requirements provide a general framework for effective system monitoring and log management procedures. It's important to tailor these guidelines to the specific needs, technologies, and compliance requirements of the organization.

- **Develop a system and data integrity management guideline.**

  - Data Accuracy: The guideline should require data to be accurate, free from errors, and reflect the true values or representations of the information it represents.

  - Data Completeness: The guideline should mandate that data is complete, meaning that it contains all the required fields, attributes, or components necessary for its intended purpose.

  - Data Consistency: The guideline should ensure that data is consistent across different systems, databases, or sources. This includes maintaining consistent formats, units of measurement, and data structures.

  - Data Validity: The guideline should require that data meets predefined validation rules and criteria. It should prevent the inclusion of invalid or unauthorized data.

  - Data Integrity Controls: The guideline should outline controls and mechanisms for ensuring data integrity. This includes implementing data validation checks, data encryption, access controls, audit trails, and checksums to detect and prevent data tampering or unauthorized modifications.

- Data Security: The guideline should address data security measures to protect data integrity. This includes implementing access controls, encryption, authentication, and other security measures to prevent unauthorized access, alteration, or deletion of data.

- Data Retention and Archiving: The guideline should define requirements for data retention and archiving to preserve data integrity over time. It should outline data retention periods, storage requirements, backup procedures, and disaster recovery measures.

- Data Audit and Monitoring: The guideline should mandate regular data audits and monitoring to identify and address data integrity issues. It should include processes for detecting and resolving data anomalies, inconsistencies, or breaches.

- Data Quality Management: The guideline should promote data quality management practices to maintain data integrity. This includes implementing data quality controls, data profiling, data cleansing, and data quality assessment processes.

- Data Governance: The guideline should incorporate data governance principles to ensure accountability and responsibility for data integrity. It should define roles, responsibilities, and processes for data stewardship, data ownership, and data governance practices.

- Compliance and Regulatory Requirements: The guideline should address compliance and regulatory requirements related to data integrity. It should align with industry-specific regulations, legal requirements, and data protection standards.

- **Develop an end-user device application management guideline.**

  - Application Inventory: Maintain an up-to-date inventory of all end user applications used within the organization. (This is related to IT configuration item management)

  - Application Approval Process: Define a process for approving new end user applications before they are deployed across the organization. This process should include assessing the application's security, functionality, compatibility, and licensing considerations.

  - Baseline Configuration: Establish a baseline configuration for authorized end user applications. This includes defining standard settings, features, and security controls that should be uniformly applied to all instances of the application.

  - Application Deployment: Develop procedures for deploying authorized end user applications to end user devices. This may involve using centralized software distribution mechanisms, automated deployment tools, or other means of ensuring consistency and control.

  - Application Updates and Patches: Establish a process for managing updates and patches for end user applications. This includes monitoring for new updates, testing them for compatibility and stability, and deploying approved updates in a timely manner.

- Application Version Control: Implement version control mechanisms to ensure that only authorized versions of end user applications are deployed and used. This helps prevent compatibility issues, security vulnerabilities, and unauthorized software installations.

- Application Access Control: Define access controls for end user applications to ensure that only authorized individuals have access to sensitive applications or specific application functionalities. This may involve user authentication, role-based access control (RBAC), or other access management mechanisms.

- Application Licensing and Compliance: Maintain proper licensing documentation and ensure compliance with software licensing agreements for all end user applications. Regularly review and reconcile software licenses to prevent unauthorized installations or violations. (Related to IT asset management guideline)

- Application Security Controls: Implement security controls appropriate for end user applications to protect against threats such as malware, data breaches, and unauthorized access. This may include antivirus software, firewalls, application whitelisting, or other security measures.

- Application Monitoring: Establish procedures for monitoring end user applications to detect any unauthorized or malicious activities. This may involve monitoring application logs and implementing intrusion detection mechanisms.

- **Develop a knowledge management procedure.**
  - Knowledge Capture and Documentation: Establish processes for capturing, documenting, and organizing IT knowledge. This includes the procedure for creating a central repository or knowledge base where information, documents, procedures, and best practices can be stored and accessed by relevant stakeholders.

  - Classification and Categorization: Develop a procedure for classifying and categorizing knowledge assets to facilitate easy retrieval and navigation. This may involve using tags, metadata, or a hierarchical structure to organize knowledge based on topics, domains, or functional areas.

  - Knowledge Creation and Validation: Define guidelines and processes for creating and validating knowledge assets. Ensure that information is accurate, up-to-date, and relevant. Encourage collaboration and input from subject matter experts to enrich the knowledge base.

  - Search and Retrieval Capabilities: Implement robust search and retrieval capabilities within the knowledge management system. Users should be able to locate relevant information using keywords, filters, or advanced search functionalities quickly and easily.

- Knowledge Sharing and Collaboration: Promote a culture of knowledge sharing and collaboration within the organization. Encourage employees to contribute their expertise, insights, and lessons learned to the knowledge base. Foster collaboration platforms, discussion forums, or wikis to facilitate information exchange and collective learning.

- Access Control and Security: Implement access controls and security measures to protect sensitive or confidential knowledge assets. Define user roles and permissions to ensure that only authorized individuals can access and modify certain information.

- Knowledge Maintenance and Update: Establish processes for regularly reviewing, updating, and maintaining the knowledge base. Assign responsibilities for periodically reviewing and validating the accuracy and relevance of knowledge assets. Implement mechanisms for users to provide feedback or suggest updates.

- Knowledge Transfer and Training: Develop programs and initiatives to facilitate knowledge transfer and training within the organization. This may involve mentoring, on-the-job training, knowledge sharing sessions, or formal training programs to ensure that knowledge is effectively disseminated and utilized.

- Integration with Other IT Processes: Ensure that the knowledge management procedure is integrated with other IT processes such as incident management, problem management, and change management. Knowledge assets should be readily available to support these processes and enable efficient problem resolution and decision-making.

- Governance and Ownership: Define governance structures and roles for overseeing the knowledge management procedure. Assign ownership and accountability for maintaining and updating the knowledge base. Establish procedures for monitoring compliance, addressing conflicts, and ensuring continuous adherence to the knowledge management guidelines.

- **Develop an IT service supply chain management procedure.**

  - Consider the reference input from already established Bank guidelines and procedures in the budget, finance, and accounting domain.

  - Budgeting and Cost Allocation: Define processes for budgeting IT services and allocating costs to the respective business units or departments. This includes establishing budgeting cycles, cost estimation methodologies, and mechanisms for tracking and reporting IT expenditures.

  - Financial Analysis and Reporting: Implement mechanisms for analysing IT costs, conducting financial performance analysis, and generating reports. This includes financial metrics, cost variance analysis, return on investment (ROI), and cost-benefit analysis. Reports should provide insights into the financial health of IT services and assist in decision-making.

- Cost Optimization and Efficiency: Establish processes for identifying cost optimization opportunities and driving efficiency in IT service delivery. This may include conducting cost benchmarking, identifying cost-saving initiatives, optimizing resource utilization, and evaluating alternative sourcing options.

- Service Management: Integrate financial management with service management processes. This involves aligning financial objectives with the organization's service portfolio, evaluating the financial viability of services, and determining the financial impact of service retirement or introduction.

- Vendor and Contract Management: Establish processes for managing vendor contracts and financial aspects of vendor relationships. This includes tracking and managing contract costs, evaluating vendor financial stability, and ensuring compliance with financial terms and conditions. (Related to vendor management guideline)

- Financial Planning and Forecasting: Develop processes for financial planning and forecasting of IT costs and investments. This includes aligning IT financial plans with the organization's strategic goals, considering future business needs, and conducting scenario planning to assess the financial impact of different investment options.

- **Develop IT technology architecture procedure.**

  - Scope and Objectives: Clearly define the scope and objectives of the technology architecture procedure. This should include the purpose of the procedure, the desired outcomes, and the key principles that will guide the development and maintenance of the technology architecture.

  - Governance and Stakeholder Engagement: Establish a governance framework that defines the roles, responsibilities, and decision-making processes related to technology architecture. Engage key stakeholders, such as business leaders, IT executives, and subject matter experts, to ensure their input and alignment with the technology architecture objectives.

  - Standards and Frameworks: Define the procedure of assessing and selecting a set of technology standards and frameworks that will be used to guide the design and implementation of technology solutions. This may include industry best practices, architectural patterns, and reference architectures. Ensure that these standards are aligned with the organization's strategic goals and industry regulations.

  - Architecture Development Methodology: Develop a methodology or framework for designing and evolving the technology architecture. This should include steps for assessing current technology capabilities, defining future state architectures, and creating transition roadmaps to guide the evolution of the technology landscape.

- Documentation and Repository: Establish the procedure of a central repository for storing and managing architecture artifacts, such as architecture models, diagrams, version controls, and design documents. Ensure that these artifacts are easily accessible, up to date, and well-documented to facilitate collaboration and decision-making.

- Integration and Interoperability: Define guidelines and principles for ensuring integration and interoperability between different technology components within the architecture, addressing the challenges of data governance, data sharing, and interoperability standards. This may include standards for data exchange, application interfaces, messaging protocols, and integration patterns.

- Security and Compliance: Incorporate security and compliance requirements into the technology architecture. Define security principles, controls, and guidelines to ensure the confidentiality, integrity, and availability of systems and data. Ensure compliance with relevant regulations, standards, and industry best practices.

- Scalability and Performance: Consider scalability and performance requirements when designing the technology architecture. Define guidelines and principles for scaling technology components, optimizing performance, and ensuring the efficient utilization of resources.

- Technology Evaluation and Selection: Establish processes and criteria for evaluating and selecting technology solutions that align with the architecture principles and strategic objectives. This may involve conducting technology assessments, vendor evaluations, and proof-of-concepts.

- Change Management and Governance: Aligned with related documents about IT Change Management, ensure the procedures for managing changes to the technology architecture. Establish a change control process that ensures proposed changes are reviewed, evaluated, and approved based on their alignment with the architecture objectives and impact on the overall technology landscape.

- Developing an electronic data retention guideline

  - Data retention guidelines are established to provide the organization with a framework for managing and storing data in a way that complies with legal, regulatory, and business requirements.

  - Compliance with regulations: Comply with applicable laws, regulations obligations and requirements from internally and externally.

- Litigation and legal proceedings: Ensure the organization retains data for a sufficient period to support legal proceedings. This includes preserving evidence for potential lawsuits, investigations, or audits.

- Business operations and decision-making: Support the organization's operations and decision-making processes. Historical data can be used for trend analysis, forecasting, performance evaluation, and strategic planning. The data retention guidelines help the organization identify what data is worth retaining and for how long to maximize its utility.

- Security and data protection: Incorporate considerations for data security and privacy. Retaining data for longer than necessary increases the risk of unauthorized access, breaches, or misuse.

FR4. Information Technology Process and Governance Documents to be reviewed and updated.

- **Review and update Information Technology Policy**
  - An information technology (IT) policy outlines the overarching rules, hierarchies, guidelines, and procedures that govern the use of technology resources within the organization. It should articulate the role, responsibilities and approval authorities in the Information Technology related process and services.

  - Acceptable Use: The policy should define acceptable and unacceptable use of IT resources by employees.

  - Data Privacy: Establish guidelines on the collection, storage, processing, and sharing of sensitive data. The policy should comply with applicable data protection laws and regulations, outline data handling procedures, and ensure data privacy and confidentiality.

  - IT Asset Management: Specify the proper use, maintenance, and disposal of IT assets, including hardware, software, and data. It may cover topics such as software licensing, asset inventory, equipment maintenance, and data backup and recovery.

  - User Responsibilities: Define the responsibilities and expectations of employees regarding the use of IT resources and BYOD. This may include guidelines on software installation, system updates, reporting security incidents, and maintaining the integrity and confidentiality of company data.

  - Network and Internet Usage: Establish guidelines on network usage, internet access, and online communication. This can include restrictions on accessing certain websites, downloading files, using external storage devices, and guidelines for remote work and accessing company resources from outside the office.

- Compliance and Legal Requirements: Address compliance with relevant laws, regulations, and industry standards. It may cover topics such as copyright infringement, intellectual property protection, software licensing, and regulatory compliance specific to the organization.

- Incident Response and Reporting: Outline procedures for reporting security incidents, such as data breaches or unauthorized access. It should define roles and responsibilities during incident response and specify the steps to be followed in the event of a security breach.

- Training and Awareness: Emphasize the importance of employee training and awareness regarding Information Technology and best practices. It should encourage regular training sessions, awareness campaigns, and provide resources to educate employees about potential risks and preventive measures.

- Enforcement and Consequences: Clearly state the consequences of policy violations and the enforcement measures that will be taken. This may include disciplinary actions, termination of employment, or legal actions if warranted.

- **Review and update Information Technology Service Management Policy**
  - Scope and Objectives: Clearly define the scope of the ITSM policy and outline its objectives. This section should establish the purpose of the policy and what the organization aims to achieve through effective IT service management.

  - Governance Structure: Define the governance structure and responsibilities for IT service management within the organization. This includes identifying key stakeholders, decision-making processes, and accountability mechanisms.

  - Service Catalogue: Define the services offered by the IT function and create a service catalogue that outlines the service offerings, service levels, and associated costs.

  - Service Level Agreements (SLAs): Establish SLAs that define the agreed-upon levels of service for each IT service provided. SLAs typically include metrics such as response times, resolution times, availability, and performance targets.

  - Incident and Problem Management: Define processes for reporting, managing, and resolving IT incidents and problems. This includes incident categorization, prioritization, escalation procedures, and root cause analysis to prevent recurring issues.

  - Change Management: Establish a change management process to control and track changes to the IT environment. This includes assessing the impact and risk of changes, obtaining appropriate approvals, and ensuring proper testing and documentation.

  - Configuration Management: Define procedures for managing and maintaining the configuration items (CIs) within the IT infrastructure. This includes tracking relationships between CIs, maintaining an accurate configuration management database (CMDB), and controlling changes to CIs.

- Service Desk: Outline the roles and responsibilities of the service desk function, including incident and request management, customer communication, and service desk performance measurement.

- Continual Service Improvement: Establish a framework for continual service improvement to drive ongoing enhancements to IT services, processes, and performance. This includes measuring key performance indicators (KPIs), conducting regular reviews, and implementing improvements based on lessons learned.

- **Review and update IT project management guideline**

  - Project Initiation: Clearly define project objectives, scope, deliverables, and success criteria. Identify stakeholders and establish project governance, including roles and responsibilities of team members, sponsors, and decision-makers.

  - Project Planning: Develop a comprehensive project plan that includes tasks, timelines, milestones, and resource allocation. Define project dependencies, risks, and mitigation strategies. Identify and engage necessary resources, both internal and external, for successful project execution.

  - Requirement Gathering: Conduct thorough requirement gathering and analysis to understand project needs and expectations. Document requirements, prioritize them, and obtain stakeholder sign-off to ensure alignment with project goals.

  - Scope Management: Establish a process to manage and control project scope. Clearly define project boundaries, document changes through a formal change control process, and communicate any scope changes to stakeholders while assessing their impact on project objectives and timelines.

  - Resource Management: Allocate resources based on project requirements and availability. Develop resource plans, identify skill requirements, and assign team members to appropriate tasks. Monitor resource utilization and adjust as needed.

  - Design and Execution: Define the procedure to effectively manage and control the design and execution steps of the project.

  - Risk Management: Identify and assess potential risks to the project, including technical, organizational, or external factors. Develop risk mitigation plans and establish processes for monitoring, controlling, and escalating risks throughout the project lifecycle.

  - Communication and Stakeholder Management: Establish a communication plan to ensure effective and timely communication among project team members, stakeholders, and

sponsors. Define communication channels, frequency, and modes of communication to keep all stakeholders informed and engaged.

- Project Tracking and Monitoring: Implement mechanisms to track project progress against the project plan. Monitor key performance indicators (KPIs), track milestones, and document project status regularly. Identify and address any deviations or delays promptly to mitigate risks.

- Change Management: Establish a formal change management process to handle requested changes during the project. Evaluate change requests, assess their impact on project scope, timeline, and resources, and obtain proper approvals before implementing changes. (Related to change management process)

- Quality Assurance: Define quality standards and establish processes for quality assurance and quality control. Conduct regular quality reviews, implement testing and validation processes, and ensure compliance with applicable quality standards.

- Documentation and Reporting: Maintain accurate project documentation, including project plans, requirements, risk registers, meeting minutes, and progress reports. Generate regular status reports, update stakeholders on project progress, and document lessons learned for future projects.

- Project Closure and Evaluation: Develop a project closure plan to ensure a smooth transition from project execution to operations or maintenance. Conduct a thorough project evaluation, including assessing project success, identifying areas for improvement, and capturing lessons learned for future projects.

- **Review and update IT service management policy and IT Operations Management Procedure**

  - Service Strategy: Define a clear and aligned IT service strategy that supports the organization's overall business objectives. This includes understanding customer needs, assessing service capabilities, and identifying opportunities for service improvement.

  - Service Design: Design IT services that meet the requirements of the business and customers. This involves creating service portfolios, defining service-level agreements (SLAs), designing service architectures, and ensuring service scalability, availability, and continuity.

  - Service Transition: Establish processes for smoothly transitioning new or changed services into the live environment. This includes change management, release management, and configuration management to ensure proper testing, documentation, and communication during service transitions.

  - Service Operation: Ensure the effective and efficient delivery of IT services on a day-to-day basis. Establish incident management, problem management, and request fulfilment processes to address service disruptions and fulfil user requests. Implement event

management and monitoring mechanisms to proactively detect and resolve potential issues.

- Service Desk and Customer Support: Establish a central service desk or helpdesk function to handle service requests, incidents, and user inquiries. Define service desk procedures, staffing requirements, escalation paths, and service level targets for effective customer support.

- Service Level Management: Define and manage service level agreements (SLAs) with customers and stakeholders. Establish processes to monitor and report on service performance, track service level achievements, and initiate actions to address any SLA breaches.

- Service Continuity and Disaster Recovery: Develop plans and procedures to ensure business continuity in the event of disruptions or disasters. Conduct risk assessments, create backup and recovery strategies, and regularly test and update these plans to minimize service downtime.

- Change Management: Establish a formal change management process to control and manage changes to IT services and infrastructure. This includes documenting and assessing change requests, evaluating impacts, obtaining approvals, and communicating changes to relevant stakeholders.

- Service Asset and Configuration Management: Implement processes to track, control, and manage IT assets and configurations. This includes maintaining an accurate configuration management database (CMDB), tracking relationships between assets, and ensuring proper configuration controls throughout the service lifecycle.

- Service Reporting and Performance Measurement: Establish mechanisms to measure, report, and review service performance. Define key performance indicators (KPIs) and service metrics, and regularly report on service performance against these targets. Conduct service reviews to identify areas for improvement and take corrective actions as necessary.

- Supplier and Vendor Management: Develop processes to manage relationships with suppliers and vendors that provide external services or support. This includes vendor selection, contract negotiation, performance monitoring, and periodic vendor reviews to ensure service quality and value for money.

- Continuous Service Improvement: Foster a culture of continuous improvement within the IT service management framework. Encourage the identification of opportunities for service enhancement, conduct regular service reviews, and implement improvement initiatives to enhance service quality, efficiency, and customer satisfaction.

- **Review and update IT change management guideline**

- Change Management Policy: Establish a change management policy that outlines the purpose, scope, and objectives of the change management process. This guideline should define the roles and responsibilities of key stakeholders involved in the change management process.

- Change Request Process: Define a structured and documented change request process. This process should include a standardized form or template for submitting change requests, as well as clear guidelines for providing relevant information such as the reason for the change, expected outcomes, and potential risks or impacts.

- Change Categorization and Prioritization: Develop a method for categorizing and prioritizing change requests based on their impact, urgency, and complexity. This helps ensure that changes are assessed and implemented in the appropriate order and that resources are allocated accordingly.

- Change Assessment and Approval: Establish a change assessment and approval process that involves evaluating the potential impact of the change on the IT environment, including infrastructure, systems, and services. This process should involve a formal review by a change advisory board (CAB) or a designated change management team responsible for assessing and approving changes.

- Change Documentation and Communication: Require comprehensive documentation of all approved changes, including details such as the description of the change, implementation plan, rollback plan, and any required testing or validation activities. Ensure that relevant stakeholders are informed about approved changes and their scheduled implementation dates.

- Change Implementation and Testing: Define procedures for implementing changes in a controlled and systematic manner. This may involve creating a change window or maintenance window for implementing changes, conducting pre-implementation testing, and coordinating with other IT teams or vendors involved in the change implementation.

- Change Review and Post-Implementation Evaluation: Conduct post-implementation reviews to assess the success of implemented changes and identify any issues or areas for improvement. Evaluate the effectiveness of the change management process and capture lessons learned for future changes.

- Change Backout and Rollback Procedures: Establish procedures for backout and rollback of changes in case they do not meet the desired outcomes or cause unexpected issues or disruptions. Define the criteria and steps for reverting to the previous state and communicate these procedures to relevant stakeholders.

- Change Management Tools: Implement appropriate change management tools or software to support the change management process. These tools can help automate change request tracking, facilitate communication among stakeholders, and provide visibility into the status and progress of change requests.

- Change Reporting and Metrics: Establish mechanisms for tracking and reporting on change management activities and metrics. This includes generating regular reports on the number of changes, their status, success rate, and any associated incidents or problems. Use these reports to identify trends, assess the effectiveness of the change management process, and identify areas for improvement.

- **Review and update IT incident management guideline**
  - Incident Management Policy: Establish an incident management guideline that outlines the purpose, scope, and objectives of the incident management process. This policy should define the roles and responsibilities of key stakeholders involved in incident management.

  - Incident Identification and Reporting: Define procedures for identifying and reporting incidents. This includes establishing clear channels for reporting incidents, such as a dedicated helpdesk or service desk, and ensuring that users are aware of how and where to report incidents.

  - Incident Categorization and Prioritization: Develop a method for categorizing and prioritizing incidents based on their impact, urgency, and business criticality. This helps ensure that incidents are addressed in the appropriate order and that resources are allocated accordingly.

  - Incident Logging and Documentation: Require comprehensive documentation of all incidents, including details such as the date and time of the incident, a detailed description of the incident, the affected systems or services, and any initial actions taken to mitigate the incident.

  - Incident Escalation and Communication: Define procedures for escalating incidents based on their severity or impact. Establish communication channels and protocols for keeping stakeholders informed about the status and progress of incidents, including regular updates on incident resolution efforts.

  - Incident Investigation and Diagnosis: Establish procedures for investigating and diagnosing incidents to determine their root cause. This may involve analysing system logs, reviewing error messages, or conducting forensic analysis to identify the underlying issues.

  - Incident Resolution and Recovery: Define procedures for resolving incidents and restoring affected systems or services to normal operation. This includes establishing response time targets, documenting resolution steps, and conducting post-incident reviews to identify opportunities for improvement.

  - Incident Closure and Documentation: Develop a process for formally closing incidents once they have been resolved. This includes verifying that the incident has been fully resolved, documenting the actions taken, and obtaining confirmation from relevant stakeholders.

- Incident Management Tools: Implement appropriate incident management tools or software to support the incident management process. These tools can help automate incident tracking, facilitate communication among stakeholders, and provide visibility into the status and progress of incidents.

- Incident Reporting and Metrics: Establish mechanisms for tracking and reporting on incident management activities and metrics. This includes generating regular reports on the number of incidents, their categorization, resolution times, and any associated impact on business operations. Use these reports to identify trends, assess the effectiveness of the incident management process, and identify areas for improvement.

- **Review and update IT problem management procedure**

  - Problem Management Policy: Establish a problem management procedure that outlines the purpose, scope, and objectives of the problem management process. This policy should define the roles and responsibilities of key stakeholders involved in problem management.

  - Problem Identification and Logging: Define procedures for identifying and logging problems. This includes establishing mechanisms for users or IT staff to report problems, as well as conducting proactive problem identification through trend analysis, incident patterns, or analysis of system logs.

  - Problem Categorization and Prioritization: Develop a method for categorizing and prioritizing problems based on their impact, urgency, and business criticality. This helps ensure that problems are addressed in the appropriate order and that resources are allocated accordingly.

  - Problem Investigation and Diagnosis: Establish procedures for investigating and diagnosing problems to determine their root cause. This may involve analysing incident data, conducting impact assessments, performing root cause analysis, or engaging subject matter experts to identify underlying issues.

  - Problem Resolution and Workarounds: Define procedures for resolving problems and implementing workarounds to mitigate their impact. This includes documenting resolution steps, developing and implementing permanent fixes, and identifying and communicating temporary workarounds to minimize the impact on users or business operations.

  - Problem Closure and Documentation: Develop a process for formally closing problems once they have been resolved. This includes verifying that the problem has been fully resolved, documenting the actions taken, and obtaining confirmation from relevant stakeholders.

  - Problem Escalation and Communication: Define procedures for escalating problems based on their severity, impact, or complexity. Establish communication channels and protocols

for keeping stakeholders informed about the status and progress of problem investigations and resolutions.

- Problem Management Tools: Implement appropriate problem management tools or software to support the problem management process. These tools can help automate problem tracking, facilitate communication among stakeholders, and provide visibility into the status and progress of problem investigations and resolutions.

- Problem Reporting and Metrics: Establish mechanisms for tracking and reporting on problem management activities and metrics. This includes generating regular reports on the number of problems, their categorization, resolution times, and any associated impact on business operations. Use these reports to identify trends, assess the effectiveness of the problem management process, and identify areas for improvement.

- Knowledge Management: By referring to the knowledge management procedure, knowledge gained during problem investigations and resolutions should be properly captured and shared.

- **Review and update IT Service Continuity Guideline (disaster recovery management guideline)**

  - Disaster Recovery Policy: Establish a disaster recovery guideline that outlines the purpose, scope, and objectives of the disaster recovery process. This policy should define the roles and responsibilities of key stakeholders involved in disaster recovery efforts.

  - Recovery Point Objective (RPO) and Recovery Time Objective (RTO): Define the acceptable levels of data loss (RPO) and downtime (RTO) for each critical IT system. These objectives determine the maximum tolerable period of disruption and guide the development of recovery strategies.

  - Backup and Restore Procedures: Establish procedures for regular backup of critical data and systems. This includes defining backup schedules, methods, and storage locations. Verify the integrity and effectiveness of backups through periodic testing and restoration exercises.

  - Recovery Strategies and Plans: Develop recovery strategies and plans for each critical IT system based on the BIA, RPO, and RTO. These plans should outline the steps and actions required to restore IT services to a functional state following a disaster or disruptive event.

  - Recovery Team and Communication: Define roles and responsibilities for the disaster recovery team, including team members' contact information and escalation procedures. Establish communication channels and protocols to ensure effective coordination and communication during the recovery process.

- Alternate Site and Infrastructure: Define the procedure to identify and establish alternate facilities or data centres that can be used in the event of a disaster. Ensure that these sites are equipped with the necessary infrastructure, such as power, cooling, networking, and security, to support the recovery efforts.

- Recovery Testing and Exercising: Conduct regular testing and exercising of the disaster recovery plans to validate their effectiveness and identify any gaps or areas for improvement. This includes both tabletop exercises and full-scale recovery tests to simulate real-life scenarios.

- Vendor and Supplier Management: Establish relationships with relevant vendors and suppliers to support disaster recovery efforts. Ensure that service level agreements (SLAs) are in place, specifying their roles and responsibilities in the event of a disaster, and regularly review and assess their capabilities.

- Documentation and Documentation Management: Document all aspects of the disaster recovery process, including plans, procedures, contact lists, configuration details, and recovery test results. Regularly update and review this documentation to ensure its accuracy and relevancy.

Non-Functional Requirements

Non-functional requirements define the technical standards and quality attributes of the system, for instance, system usability, effectiveness, security, scalability, etc.

NF1.	Location

Details Service resource to work with NDB HQ staff.

Priority High

NF2.	Language

Details English is mandatory as the medium of communication and documentation

Priority High