Appendix 2

TERMS OF REFERENCE

on conducting an audit of information technology
of the National Bank of Tajikistan

June, 2023
Dushanbe, Tajikistan

I. Terms and definitions

- Customer – National Bank of Tajikistan, NBT,
- Contractor - external audit organization
- Information security management system - part of the overall management system of the organization and a set of internal organizational and administrative documents and resources necessary to protect the assets of the Customer; provides conscious decision-making in the field of information security (IS) through mechanism of managing business risks in the creation, implementation, operation, monitoring, analysis, support and improvement of IS.

II. Rationale

The purpose of an audit is to check information systems, security systems, and IT management processes in general for compliance with both the company's business processes and international standards. This procedure is necessary in order to assess the correctness of IT development based on international experience, as well as approve and document the decisions made.

It allows to direct the activities of the IT department to achieve a new level of IT development in accordance with international standards. Compliance testing can help identify non-obvious inconsistencies in IT with accepted standards and thereby justify the need to make appropriate amendments, as well as identify which processes or systems are not functioning efficiently and are “bottlenecks” for IT operations as a whole.

IT audit allows to assess the compliance of information systems with business requirements and build a long-term strategy for the development of information technology. In addition, the reason for conducting an IT audit is the need to identify potential risks and bottlenecks in the IT infrastructure. Only an IT audit can confirm the compliance of systems and business processes with international standards, which is necessary for any company, especially banks.

III. Audit tasks

The purpose of the Bank in conducting a system audit of information systems and IT infrastructure is to obtain reasonable assurance from a third-party auditor that:

- The Bank's information systems and data are protected and will remain complete, integrated, up-to-date and accurate throughout processing.
- Information assets/resources of the Bank (hardware/software) protected from unauthorized access/use/damage/change.
- A bank's business continuity planning is adequate to ensure uninterrupted customer service despite interruptions in facilities for a significant period.
- Bank networks are properly secured and secured.
- The bank's computer operations are carried out in a controlled environment.
- The Bank may obtain an independent assurance of the effectiveness of controls maintained by third party technology service providers (Facility Management Service Provider).

- The Bank has appropriate controls throughout the life cycle of systems development, project management and implementation activities.
- The Bank complied with all the necessary legal requirements.

IV. Audit area

The scope of the audit should cover the business processes of the NBT and their respective information systems, software, communication systems and network infrastructure, regulations and management protocols for the implementation of IT services provided to internal users of the Customer and external organizations (banks, microfinance institutions, insurance companies, government agencies and other agencies, etc.).

As part of the audit, the Contractor shall evaluate the current state of the information security management system and IT infrastructure of the NBT, as well as identify risks and opportunities:

1. Vulnerability assessment of infrastructure related to the CBS network, data center, disaster recovery site, CBS back office, head office, regional offices and branch offices, etc.
2. Functioning of the back office CBS & Data Center/ DR. Audit covering user / help desk / settings / access / internal repairs/ change management, etc.
3. System audit of the main banking applications, including the main application. The broad areas to be covered are indicated in ***Appendix - I.***
4. Network audit, NMS (network monitoring system) and administrative process with report and recommendations. The broad areas to be covered are specified in ***Appendix - II***.
5. Report on capacity management and performance tuning of the entire CBS architecture with recommendations, if any, to improve performance and security. The broad areas to be covered are specified in ***Appendix - III*** .
6. Audit CBS processes focusing on critical areas such as password control, user ID control, operating system security, anti-malware control, manufacturer verification control, segregation of duties, staff rotation, physical security, viewing exception reports/audit logs, business continuity and testing policies, etc.
7. Conduct a vulnerability assessment and system audit of information systems of standard applications and legacy applications (either integrated with CoreBankingSolution or running standalone), such as:
   - Payment channels, for example. ATM, Mobile banking, UPI
   - RTGS, Reuters Dealing, CSD, 1C - Enterprises, NPCR, SWIFT, etc.
8. An overview of current security measures and recommendations for their improvement.
9. Disaster Recovery Site Audit (Disaster Recovery):
   - Checking systems/controls;
   - Assessment of the environment and procedures;
   - Evaluation of control parameters;
   - Infrastructure adequacy (ability to handle full traffic);
   - Review of back-up procedures;
   - Access Control Assessment.
10. Records management / Recording processes and controls:
    - Media Handling, Disposal and Transit Policy;

- Periodic review of authorization levels and mailing lists;
- Procedures for handling, storage and disposal of information and media;
- Storing backup media ;
- Protect records from loss, destruction and falsification in accordance with legal, regulatory, contractual and business requirements.

11. Vulnerability assessment and penetration testing (VAPT) for the entire IT ecosystem, including the bank's information system infrastructure (network systems, security devices, servers, databases, application systems accessible via WAN, LAN, and also with public IPs -addresses, bank website and supplier-hosted email server). The auditor is expected to identify existing threats and vulnerabilities and propose corrective solutions and recommendations on them to mitigate all identified risks in order to improve the security of information systems.
12. Auditor's comments /recommendations on various training and knowledge improvement programs.
13. Develop a package of recommendations for preparing the information security management system of the NBT for certification in accordance with the requirements of one of the international information security standards;
14. Assess the Customer's readiness for certification of the information security management system implemented in the NBT for compliance with one of the international information security standards;

Data collection:
Contractor shall conduct the actual collection of relevant data and information that is necessary to evaluate the information security management system process; and ensure the consistency of data and information, and the interpretation of results.

Privacy:
Contractor shall maintain the confidentiality of the information collected for the project. Thus, disclosure of data or any related information requires the consent of the NBT.

Intellectual property:
All intellectual property, including studies, reports or other materials, models, spreadsheets, belongs to and remains the property of the NBT.

V. Responsibilities of the Customer

The Customer must assist the contractor in conducting an audit of its IT system by providing and ensuring the following:
1) Coordination with the relevant structures of the NBT (regional offices, departments, managements, NBT divisions, etc.) regarding all the necessary information;
2) Technical and administrative support of the work, such as organizing meetings, interviews, presentations and other related events.

VI. Responsibilities of the Contractor

The Contractor should perform procedures mentioned in part IV. The Contractor must have the following experience and competence:

1) to have relevant experience in the field of service delivery and audit of IT system;
2) to have relevant knowledge, experience and capabilities to implement this project. The group of auditors should include specialists with good knowledge in the field of information security management systems, international information security standards;
3) be able to communicate with NBT employees and other interested parties, as well as have access to the necessary documents for the performance of services, including documentation in English on the international information security standard chosen by the NBT.

VII. Deadlines and results

Term for completion of IT audit work and provision of an audit report is determined by the contract.

APPENDIX I

Scope of the system audit of the Core Banking Solution (" CBS ") software:

- Input controls;
- Processing management;
- Output management;
- Logical access control;
- Controls the automated processing/updating of records, reviewing or verifying important calculations such as interest rates, repayment schedule, etc., reviewing the operation of automated scheduled tasks, developing output reports, distributing reports, etc;
- Ability to audit both client-side and server-side, including sufficiency and accuracy of event logging, use of SQL prompt commands, database-level logging of all other interfaces with other applications, etc;
- Degree of parameterization;
- Functionality;
- Internal controls embedded at the application software level, database level, server and client side;
- Backup/Rollback/Restore procedures and contingency plannin;
- Proposed segregation of roles and responsibilities for application software to improve internal controls;
- Overview of formal naming standards documentation, process for developing worker roles, activities, groups, and profiles, assigning, approving, and periodically reviewing user profiles, and assigning and using superuser access;
- Manageability in terms of ease of setup, rollback of transactions, time required to end the day, start operations, and restore procedures;
- Special remarks may also be made on the following points:

  Hard-coded user ID and password, EDI, web server and other network-level, application-level interfaces. Recovery and restart procedures. Sufficiency and coverage of UAT test cases, review of UAT defects and tracking mechanism deployed by the vendor, and resolution, including retesting and acceptance Overview of the customizations made to the software, and the SDLC policy that such customization follows. Suggested procedure for managing changes during conversion, data migration, version control, etc.
- Suggest any application-specific auditing tools or programs;
- Review of software test results, load, and stress testing of IT infrastructure performed by vendors;
- Adequacy of audit logs and meaningful logs;
- Compliance with legal and regulatory requirements;
- Setting up system mail;
- Adequacy of anti-virus measures in the CBS environment;
- Adequate protection of all servers (data center and branch offices) and verification of application of the latest patches provided by various vendors for known vulnerabilities published by CERT , SANS , etc.;
- In addition to the Application Software System Audit, the System Audit must be conducted at the Data Processing Center, at the disaster recovery site, at the head office and regional office;

APPENDIX II

Scope of system audit of network infrastructure components, networks and application security:

- Network Scanning - Threat and Vulnerability Assessment: This is the process of measuring and prioritizing risks associated with network and host systems and devices in order to rationally plan technology and business risk management activities;
- Password cracking;
- Intrusion Detection System / Intrusion Prevention System Testing;
- Testing Firewall;
- Router testing;
- Denial of Service Testing (DOS);
- Distributed DOS testing;
- Testing containment measures;
- When performing a penetration test on servers in a real environment, ISA must ensure that systems perform optimally;
- Verification of network monitoring software (NMS) installed to monitor critical servers of the entire network, including branch offices, for sizing, etc., for monitoring LAN and WAN network components, fault management, network performance management, inventory management, automatic detection from network components, etc. NMS is also implemented to proactively monitor, report, and report on the performance of the core-banking network. This functionality needs to be tested and verified;
- Network Infrastructure Overview: Network Infrastructure at Branches, CBS - Project Office , Data Center, DR Site , and NAP (Network Aggregation Points);
- Network management analysis. Key aspects of management need to be reviewed, such as standards for equipment, applications, capacity planning, performance, reporting, problem solving, costing and accounting;
- Network administrative check:
  - Domains to check for effective network administration;
  - Monitor structured cabling and network usage;
  - Tuning optimization;
  - Eliminate bottlenecks;
  - Bandwidth allocation (demand/usage, especially during peak hours for large/service branches);
  - Standard reports and troubleshooting steps;
  - Efficiency and security of data transfer;
- Data transfer:
  - Packet size of transmitted message;
  - Message transfer rate. The security of message packets to be transmitted, whether or not they are protected from unauthorized access. Adequacy of encryption procedures for transmitted data;
  - FTP and SFTP file transfer protocol;
- Network security audit:
  - It is necessary to review the physical and logical security measures, tools and processes implemented to protect against unauthorized entry into the corporate network. Firewall and router configuration, the effectiveness of an intrusion detection system, and/or

automatic auditing of all network users are key areas that should be checked. Check whether adequate security is provided in the various network connections to ensure that only authorized users can access the system;
  - Check if remote login is enabled, and if so, if it can be identified by terminal IDs/ IP addresses;
  - Check if remote login via services like ftp, telnet, etc. is disabled. If not, make sure the same has been implemented as instant recommendations;
  - In the case of WANs (wide area networks), whether the router is securely serviced to ensure efficient system administration;
  - The focus should be on discovering system vulnerabilities that arise from multiple levels of access. Standard tools should be used to scan various network entry points and a comprehensive analysis of the security objectives should be provided. The scope includes the operating system, databases, firewalls, routers, remote access devices, and switches;
  - Review the actions of the network administrator/system administrator and suggest improvements and controls, if any;
- Security device audit:
  - Configuration, policy/rule sets, signatures, validation, logging, location, redundancy, port restrictions, patches and updates, administration and management;
  - Firewalls (Juniper/CISCO and FortiGATE);
  - Network intrusion prevention systems;
  - Intrusion Detection Systems;
- Architecture and Placement of Security Devices:
  - Change Management Processes - Deploy rules, policies, and change management adequacy with a fault logging tool;
  - Incident Management Processes;
  - Documentation;
  - Adequacy of monitoring/ anti-phishing services;
  - Adequacy of security monitoring;
  - Failover/failover processes and testing of failover/failover processes;
- Adequacy of reporting and escalation mechanisms;
- Patch Management.

APPENDIX III

System Audit Scope of Power Management and Performance Tuning

The purpose of a capacity planning and management audit is to assess whether satisfactory levels of service are provided to users in a cost effective manner.
An overview of the following functions performed by the Bank's IT division:

- Defining service level requirements;
- Current power analysis;
- Analysis of network bandwidth availability at the peak level;
- Planning for the future;
- Periodic review of workloads and services;
- Measuring total resource usage;
- Defining the process for measuring incoming work;
- Establish service level requirements versus performance;
- Checking if the organization will be ready for the future.