BANK OF UGANDA

OFFICE OF
THE EXECUTIVE DIRECTOR
SUPERVISION

37-45 KAMPALA ROAD,
P.O. BOX 7120,
KAMPALA

DIRECT LINE	256-414- 230051
GENERAL LINE	256-414- 258441 Ext 2403
FAX LINE	256-414- 258515
TELEX	256-414-61059
CABLES	UGABANK
Email	info@bou.or.ug
Web site	www.bou.or.ug

EDS.306.2

July 13, 2017

Circular to all Chief Executives of Commercial Banks, Credit Institutions and Microfinance Deposit-taking Institutions

External Audit of Information and Communication Technology Systems of Supervised Financial Institutions

In the recent past, Information Technology (IT) has become a key business enabler for Supervised Financial Institutions (SFIs) and has increasingly become an integral part of the institution's business strategies, operations and service delivery. This has heightened SFIs' exposure to cyber risks hence necessitating the establishment of enhanced risk management systems in SFIs to mitigate the associated risks.

To this end, the IT systems must be robust to effectively support the SFIs' pursuit to achieve their strategic objectives and to generate accurate financial information as well as management of reports. Whereas Bank of Uganda (BoU) reviews the adequacy of IT systems in SFI's during on-site examinations, it is deemed necessary that we obtain additional assurance from IT experts on the capacity of these IT systems to safeguard assets and maintain data availability, integrity and confidentiality.

In view of the above, and in accordance with Section 69 (4) of the Financial Institutions Act, 2004, Bank of Uganda hereby directs SFIs to engage their appointed External Auditors to audit the IT systems of the respective SFIs starting this financial year and subsequently **at least once every two years**. The initial audit shall be conducted immediately and the reports must be submitted to BoU by **October 31, 2017.** Thereafter, the IT audits shall be conducted as at **end of December** of the period under review and the reports must be submitted to Bank of Uganda by **end of March** of the following year together with the end of year financial statements.

Please note that the External Auditors are required to deploy IT specialists for these audits whose profiles must be submitted to Bank of Uganda by **August 31, 2017** and subsequently every **end of July** of the year of Audit.

The cost of these IT audits shall be borne by the respective SFIs.

We have attached the scope of these IT audits which should act as a **minimum** guidance.

J. Bagyenda (Mrs.)
Executive Director Supervision

Attach...

PROPOSED MINIMUM SCOPE FOR IT AUDITORS DURING EXTERNAL AUDIT OF FINANCIAL INSTITUTIONS

NO.	AREA OF REVIEW	SUMMARY OF MINIMUM PROPOSED AREAS TO BE CONSIDERED FOR REVIEW
1.	Review all Information Communication Technology (I.C.T) Systems within the Financial Institutions including Core Banking System, operating system, applications, databases, servers and networking systems and confirm whether they are robust to ensure data integrity, confidentiality and availability and support the Institution's strategy.	a. Establish whether there are adequate policies on ICT systems and confirm whether they were approved by the Board and are regularly reviewed to accommodate changes in the Institution's business environment. b. Review the I.C.T. policies in place against best practice requirements for adequacy. c. Assess whether the policies give clear direction on the management, utilization, monitoring and security of I.C.T. resources in the bank. d. Review the structure, staffing of the ICT Function/Department, staff qualifications **(a minimum of a degree in ICT is required)** and experience to ascertain whether it is well suited to support the Financial Institution's operations in relation to the size of the Institution. e. Review the policy and procedures to guide controls around authentication and identification into the systems. f. Assess adequacy of controls in place around user account creation and termination, user authentication into system, privileged user account management and segregation of duties management. g. Review the activity of the respective accounts and investigate any anomalies for any inappropriate access noted. h. Assess A.A.A. (Authentication, Authorization and Accounting) mechanisms for Electronic Banking Systems against best practice requirements i. Review availability of systems to assess whether there is a high system availability, adequate capacity, reliable performance, fast response time, scalability and swift recovery capability.
2.	Review the Financial Institution's Procurement process to ascertain whether the Institution got value for money during the purchase of new or upgrading of the existing ICT systems.	a. Establish whether competitive procurement was done and whether it complied with the Institution's existing policies or best practice. b. Assess the extent of Board involvement in the changing or upgrading of the ICT system and ascertain whether Senior Management obtained Board approval in the various phases of the procurement process.

		c. Review the change management process to ascertain that changes to ICT systems were assessed, approved, implemented and reviewed in a controlled manner. d. Review the adequacy of the implementation process and ascertain whether at roll out of the new system, the user needs requirements were met. e. Establish whether the Board approved the budget for the purchase or upgrade of the various systems and ascertain whether the actual costs were within budget. f. Review the reasonableness of the costs incurred for purchase, deployment and maintenance of the various ICT systems in the Financial Institution
3	Perform application controls testing which include configuration controls, sensitive access and segregation of duties controls, interface controls, data integrity controls and obtain reasonable assurance on the accuracy and completeness of reports	a. Review the Bank's system change control procedures for adequacy as per best practice requirements b. Test the controls in place for system change implementation as well as operating effectiveness of the controls for changes implemented in the key applications and databases for the period under review. c. Review all changes made to the core banking system, financial reporting system , all systems interfaced with both, databases, operating systems, I.C.T. infrastructure and network components and assess whether they were logical and approved in line with bank's change controls and whether they were implemented as approved. d. Review whether the bank's applications, databases operating systems and devices are fully patched against vulnerabilities. e. Review key bank transactional processes around Electronic Banking applications system for adequacy of input and output controls. f. Assess data integrity, completeness and accuracy of the business transactions affecting the key balances i.e loans and advances, customer deposit liabilities, payments and money transfer and treasury. g. Review adequacy of service level agreements and information security controls for outsourced services supporting alternative banking channels such as mobile banking, A.T.M.s service, internet banking, agent

		banking. h. Review interfaces that support data transfer to and from the core banking system to ensure: • There is adequate segregation of duties over data origination, data input and data processing. • Data input into the system is validated • Transactions are reconciled against source data for accuracy. i. Identify non automated interfaces that pose a risk for unauthorized data manipulation j. Assess error handling capabilities (ability to detect erroneous data exchanges and flag the same) for system interfaces. k. Assess timely transfer and synchronization of data transferred across system interfaces l. Assess access controls for systems to prevent unauthorized manipulation of data transferred across system interfaces
4.	Review and assess whether balances resulting from all transactions and data processed within the institution's I.T. system are accurately captured and reported in the institution's general ledger, the financial statements and returns submitted to the Bank of Uganda	a. Review the transactions processed in the Core Banking System against balances recorded in the General Ledger for key balances i.e Loans and Advances, Customer Deposits, Payments and Money Transfer and Treasury for completeness and accuracy. b. Review on a sample basis the accuracy and completeness of BOU returns and check for adherence to the FIA, 2004 and its implementing regulations paying attention to the following; • Risk classification of loans and advances and provisioning. • Suspension of interest on NPAs. • Aggregation of credit exposures to a single person or persons with a common interest. • Integrity of the Deposit Listing and Fixed Asset Register c. Review how underlying data, used in generating the regulatory reports is generated from the associated systems.

		d. Assess any manual interventions to support the reporting process and how these may impact the completeness and accuracy of the data e. Assess the compilation and review process over the report generation procedures f. Assess the adequacy of automated customer application banking controls as designed, implemented and their ongoing effectiveness with regard to the following; • Computation of interest income, penalty fees and expenses • Reasonableness of the penalty fees charged from customers. • Security of product design parameters e.g. interest rates, tenure • Aging and classification of loans • Account dormancy management • Suspension of interest for NPLs • Application of standard charges • Computing and posting foreign exchange gains/loss • Loan portfolio review • Assessment for inappropriate insider lending • Detailed reviews of loan aging reports
5.	Review I.T. security controls including application security, privileged access, audit trails, system monitoring and maintenance, integrity and systems ability to recover from a disaster resulting into loss of data.	a. Review whether the audit logging capabilities had been enabled in the applications, databases, operating systems and networks in the period under review b. Assess whether the audit logs are monitored on a periodic basis to detect unauthorized and inappropriate activities. c. Assess adequacy of the audit logging capabilities to verify that all relevant transactional data and system user activity is captured including activities of system administrators and senior management d. Assess whether proper Start of Day is maintained in the review of the audit logs

		e. Analyze audit logs and any other key transactional data on a sample basis against a pre-set criteria to identify and investigate unusual activity within the core banking systems and the peripheral applications. f. Review the adequacy of procedures in place to manage job scheduling, data center, physical security, data backup and recovery as well as network monitoring and security. g. Review controls to ensure accurate and complete execution of batch processes and scheduled tasks e.g End-of-day/close-of-business procedure h. Assess access controls over the amendment of job scheduling and the processing parameters i. Assess adequacy of network design to ensure enhanced security e.g proper segmentation, continuous monitoring, firewalls etc. j. Review the anti-virus systems in place to guard against malicious malware and viruses k. Assess whether the antivirus software is up-to-date and covers all systems in the Institutions IT landscape. l. Assess whether anti-malware and anti-virus are applied to hand held Bring Your Own Device (BYOD) devices as well as any third party networks the Bank is connected to. m. Assess the adequacy of the Institution's Business Continuity Management program. n. Verify that the Financial Institution has in place and is operating from an in-country Primary Data Centre. In addition, verify that the Institution has in place an in-country Disaster Recovery Site, test its functionality and confirm whether there is real time replication of data between the primary and back up servers. o. Assess whether the BCM program has been tested in the period under review. p. Assess whether the BCM program has in place ICT Disaster Recovery Components. Assess whether ICT Disaster Recovery Plan has adequate recovery procedures outlined for all critical systems and component within the bank's ICT landscape. q. Ascertain whether the Institution's branches regularly test the operability of their Disaster Recovery Sites. r. Ascertain whether a vulnerability test to assess adequacy of controls to prevent external attacks on the ICT

		systems including cyber-attacks has ever been done; if not, conduct one. The Financial Institution should thereafter conduct a system penetration test every three years to cater for vulnerabilities arising from upgrades.