Appendix 1

ICT review program as per the Bank of Uganda / Summit Consulting Ltd tools.

Our ICT audit program is aligned to the regulatory requirements specifically BOU. Please provide the requested documents in full to facilitate swift execution. Only BOU areas that relate directly to ICT Security have been considered.

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
3.1	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	**1. <u>IT policies and procedures</u>** 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	*Company ICT policy and procedures documentation*	*Assessing and enumerating threats to the integrity, confidentiality, and availability of the bank's IT systems and data as per the company's ICT policy and procedures.*	
		b. Review the ICT policies in place against best practice requirements for adequacy	*-do-*	*Examine the compliance of your bank policies against COBIT, ITIL, ISO27001 and other best practices.*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
	they are robust to ensure data, integrity, confidentiality, and availability and support the Institution's strategy.	c. Assess whether the policies give clear direction on the management, utilization, monitoring, and security of ICT resources in the bank.	*IT strategic plan and investment plan*	*Assess justification for IT use, spending and security budgets*	
		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.	*Company's organization chart for ICT and Human Resource Data*	*Evaluate technology and ICT functions staff qualifications for robustness and efficiency.*	
		e. Review the policy and procedures to guide controls around authentication and identification into the systems.	• *Roles and access control documentation.*	*Assessing access using both authenticated and unauthenticated procedures.*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		2. <u>User access management</u> a. Assess the adequacy of controls in place around user account creation and termination, user authentication into the system, privileged user account management and segregation of duties management.	• *Roles and access control documentation, active directory and inventory documentation* • *Policies over user lifecycle management.*	*Assess the adequacy of controls over user management*	
		b. Review the activity of the respective accounts and investigate any anomalies for any inappropriate access noted	*Roles and access control documentation, active directory and inventory documentation*	*Examine compliance*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		c. Assess A.A.A. (Authentication, Authorization, and Accounting) mechanisms for Electronic Banking Systems against best practice requirements	*Roles and access control documentation, active directory and inventory documentation over electronic banking*	*Assessing the authentication mechanisms in place against best practice and requirements, password strength and authentication bypass to measure against modern authentication best practices*	
		d. 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.	*Systems, applications, and network documentation* *List and details of systems in use – list of servers, services running, and IP*	*Run performance and system stress testing assessments to gauge the impact on availability, reliability, and response.*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
3.3	Perform application controls testing which includes configuration controls, sensitive access and segregation of duties control, interface controls, data integrity controls and obtain reasonable assurance on the accuracy and completeness of reports	**3. <u>Change management controls</u>** a. Review the Bank's system change control procedures for adequacy as per best practice requirements.	*Systems, applications, and network documentation*	*Examine change control procedures against best practices in context*	
		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.	*Systems, applications, and network documentation* *Change Management and Control Documentation*		
		c. Review all changes made to the core banking system, financial reporting systems, all systems interfaced with both,	*Systems, applications, and network documentation*		

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		databases, operating systems, ICT 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.	*Change Management and Control Documentation*		
		4. <u>Patch management controls</u> a. Review whether the bank's applications, databases operating systems, and devices are fully patched against vulnerabilities.	*Systems, applications, and network documentation* *Change Management and Control Documentation*	*Scan and manually test the bank's systems for vulnerabilities and patch levels as per the versions documented by the bank*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		5. <u>Electronic Banking application control reviews</u> a. Review key bank transactional processes around Electronic Banking applications system for the adequacy of input and output controls	*Core Banking System Documentation*		
		d. 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.		*Assessing data security elements like encryption and.* *Authorization and roles assignment checks to check for data access violations or misconfigurations*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		6. <u>Service level management</u> a. 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 services, internet, banking, agent banking.	*Third-party applications & contractors documentation.* *Service level agreements contracts and documentation.*	*Review third party applications and the level of integration provided to the overall bank ICT system in order to determine the importance of service level agreements in place*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		7. <u>Interface controls</u> a. 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 • Transaction are reconciled against source data for accuracy	*Applications documentation, network structure, and documentation* *Network diagram showing all inter-connecting systems on the entire network*	*Examine the adequacy of controls*	
		b. Identify non-automated interfaces that pose a risk for unauthorized data manipulation	*Asset register, showing all applications,*	*Identify assets that are part of assets that are non-automated.*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
			system and network logs. Device and application inventory		
		c. Assess error handling capabilities (ability to detect erroneous data exchanges and flag the same) for system interfaces.	*Applications, system, and network logs –for though analysis*	*Examine to identified capabilities*	
		d. Assess timely transfer and synchronization of data transferred access systems interfaces	*Applications, system and network logs.*	*-do-*	
		e. Assess access controls for systems to prevent unauthorized manipulation of data transferred across system interfaces.	*Applications, system and network logs.*	*-do-*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
3.5	Review I.T security controls including application security, privileged access, audit trails systems monitoring and maintenance, integrity and systems ability to recover from a disaster resulting in loss of data	**8. <u>Audit, logging, and monitoring</u>** a. Review whether the audit logging capabilities had been enabled in the applications, databases, operating systems and network in the period under review	*Applications, system and network logs.* *Applications, system and network documentation.*	*Review and analyze logs and logging system, and adequacy of logging and storage.*	
		b. Assess whether the audit logs are monitored on a periodic basis to detect unauthorized and inappropriate activities.	*Network infrastructure documentation*	*-do-*	
		c. Asses adequacy of the audit logging capabilities to verify that all relevant transactional data and system user activity is captured including activities of system	*Applications, system, audit and network logs.*	*-do-*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		administrators and senior management			
		d. Assess whether proper Start of Day is maintained in the review of the audit logs	*The banking system, audit and network logs*	*-do-*	
		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	*Applications, system, audit and network logs.*	*-do-*	
		9. <u>IT Operations</u> a. Review the adequacy of procedures in place to manage job scheduling, data center, physical security, data backup	*IT operations documentations over scheduling, physical security, and network management*	*Review adequacy of policies over IT operations and governance*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		and recovery as well as network monitoring and security.			
		b. Review controls to ensure accurate and complete execution of batch processes and scheduled task e.g. End- of-day/close-of-business procedures	*Copy of the end of day business procedures* *Applications, system, audit and network logs.*	*Review controls to ensure accurate and complete execution of batch processes and scheduled task*	
		c. Assess access controls over the amendment of job scheduling and the processing parameters	*Access controls over job scheduling report*	*Review access controls over job scheduling*	
		10. <u>Network security</u> a. Assess the adequacy of network design to ensure enhanced security e.g. proper segmentation,	*Network architecture documentations* *Computer Security policy and*	*Examine network security adequacy*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		continuous monitoring, firewall etc.	*procedures documentation.*		
		11. <u>Antivirus management</u> a. Review the anti-virus systems in place to guard against malicious malware and viruses	*List of all security software including anti-virus systems*	*Review anti-virus and security systems for adequacy re new anti-virus definitions*	
		b. Assess whether the anti-virus software is up-to-date and covers all systems in the Institution's IT landscape.	*Devices and applications inventory management documentation*	*Review anti-virus and security systems for adequacy re new anti-virus definitions*	
		c. Assess whether anti-malware and anti-virus are applied to handheld Bring Your Own Device (BYOD) devices as well	*Third-party devices use policy and cloud applications*	*-do-*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		as any third-party networks the Bank is connected to.	*documentation i.e. BYOD policies*		
		12. <u>Business continuity management</u> a. Assess the adequacy of the Institution's Business Continuity Management program.	*Copy of the Continuity Management Program in place*	*To assess adequacy*	
		b. Verify that the Financial Institution has in place and 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	*Evidence of in-country primary data center – location. Also, obtain information on the in-country DRS* *Devices and applications inventory management documentation*	*The team will visit the center to physically confirm. Review the other in-country disaster recovery site.*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		primary and backup servers	*Third party devices use policy and cloud applications documentation*		
		c. Assess whether the BCM program has been tested in the period under review	*Business Continuity Management end of test reports*	*Assess recovery readiness during the period under review*	
		d. 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 Banks' ICT landscape.	*Business Continuity Management Documentation and previous audit documentation / Reports.* *Provide evidence of BCP tests*	*Assess the adequacy of BCP*	

NO.	Area of Review	Details of the areas to review	*Documents required*	*Work to be done*	Comments
		e. Ascertain whether the institution's branches regularly test the operability of the Disaster Recovery Sites.	*Business Continuity Management Documentation and previous audit documentation / Reports.*	*Review adequacy of disaster recovery across the bank*	
		13. <u>Vulnerability assessment</u> a. Ascertain whether a vulnerability test to assess the adequacy of controls to prevent external attacks on the ICT systems include 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 rising from upgrades.	*Devices and applications inventory management documentation* *Third-party devices use policy and cloud applications documentation*	*-do-*	

Other services we do

1) Black box pen test (fee negotiable)
2) While box pen test (fee negotiable)
3) IT governance review
4) Revenue assurance and business intelligence (for real time monitoring)

Contact us

Summit Consulting Ltd **|** *Forensics.* ***Advisory.*** *Security*

4th Floor, Ntinda Complex

Plot 33, Ntinda Road Opp St Luke Church,

P.O. Box 40292, Kampala, Uganda

M: +256 782 610333

strategy@summitcl.com