REGISTRAR OF FINANCIAL INSTITUTIONS

GUIDELINES ON INFORMATION AND CYBERSECURITY RISK MANAGEMENT FOR BANKS

October 2019

TABLE OF CONTENTS

PART I: INTRODUCTION

Information Technology (IT) innovations have significant impact on the way banks interact with their customers, suppliers and counterparties, and how they undertake their operations. Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks and other technology-related solutions to drive their businesses.

Information Technology is no longer a support function within a bank but a key enabler for business strategies, as they rely increasingly on it and the Internet to operate their business and interact with the markets. Banks are deploying advanced systems, including internet banking systems, cloud based solutions, mobile banking and payment systems to reach their customers.

In this networked environment, it is critical that banks fully understand the magnitude and intensification of information and cyber security risks from these systems. Information and cyber security risk, if not properly managed has the potential to cause disruption to the financial institution and industry at large. This could result in denial of service to customers, exposure of private information, deletion of or tampering with customers' and banks' records, and inability to manage both its own as well as customers' assets. Invariably, evidence of information and cyber security risk erodes public trust and damages the bank's reputation.

In this regard, the Registrar of Financial Institutions in Malawi ("The Registrar") has issued these guidelines to help banks to effectively manage information and cyber security risk. The Guidelines outline minimum requirements and banks are therefore expected to put in place more robust measures for managing information and cyber security risk in addition to those stipulated in these guidelines.
The Information and Cyber Security Risk Management Guidelines ("the Guidelines") supplement the Operational Risk section of RBM's Risk Management Guidelines, 2007 and will replace the Information Technology Risk Management Guidelines, 2016.

The Guidelines are issued pursuant to *Section 96* of *the Financial Services Act, 2010* and shall apply in addition to all other Risk Management Guidelines issued by the Registrar.

PART II - OBJECTIVES

The objectives of the guidelines are to:

1. Provide minimum requirements on management of information and cyber security risk.

2. Strengthen banks' information system security and protection of critical information infrastructure.

3. Promote banking industry compliance with appropriate technical and operational cyber security standards and international best practices.

4. Promote safe, sound and continuously improving information security governance and risk management practices for banks in Malawi.

5. Maintain public trust and confidence in banking system.

PART III – DEFINITION OF TERMS

"access control" means to ensure that access to assets is authorized and restricted based on business and security requirements;

"asset" means something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation;

"compromise" means Violation of the security of an entity;

"cyber" means relating to, within or through the medium of the interconnected information infrastructure of interactions among persons, processes, data and information systems;

"cyber incident" means a cyber event that: jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or violates the security policies, security procedures or acceptable use policies whether resulting from malicious activity or not;

"cyber resilience" means the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incident*s;

"cyber risk" means the combination of the probability of cyber incidents occurring and their impact;

"cyber security" means preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as *authenticity*, *accountability*, *non-repudiation* and *reliability* can also be involved;

"cyber threat" means a circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security;

"information system" means set of applications, services, information technology *assets* or other information-handling components, which includes the operating environment;

"integrity" means property of accuracy and completeness;

"patch management" means the systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs;

"penetration testing" means a test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system;

"recover" means to develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired due to a cyber incident;

"Recovery Point Objective" means the maximum time period during which data can be lost in case of an incident;

"Recovery Time Objective" means the maximum time within which a system or process must be restored after an incident;

"Reference Architecture" means the overall design and high-level plan that describes an institution's implementation framework;

"vulnerability" means a weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats;

"Vulnerability Assessment" means systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

PART IV – REGULATORY REQUIREMENTS

1. INFORMATION AND CYBER SECURITY RISK GOVERNANCE

1.1 The Board

The board shall-

1.1.1 oversee information and cyber security risks and ensure that the organization's IT function is capable of supporting its business strategies and objectives.

1.1.2 review and approve an IT strategic plan that aligns with the overall business strategy and includes an information and cyber security strategy;

1.1.3 review and approve Information and Cyber Security Risk Management Framework and associated policies.

1.1.4 approve an IT planning or steering committee, which should oversee whether IT resources are used effectively to support business strategies.

1.1.5 oversee processes for approving the bank's third-party providers, including the third parties' financial condition, business resilience, and IT security posture;

1.1.6 oversee and receive updates on major IT projects, IT budgets, IT priorities, and overall IT performance. The board may need to approve critical projects and activities.

1.1.7 ensure adequacy of IT resources for funding and personnel;

1.1.8 hold management accountable for identifying, measuring, and mitigating Information and cyber security risks;

1.1.9 provide for independent, comprehensive, and effective audit coverage of IT controls; and

1.1.10 promote high ethical and integrity standards, and a culture that emphasizes and demonstrates to all levels of personnel the importance of Information and cyber security risk management.

1.2 Senior Management

Senior management of a bank shall-

1.2.1 design an effective Information and Cyber Security Risk Management Framework;

1.2.2 implement and review an effective Information and Cyber Security Risk Management Framework and associated policies approved by the board;

1.2.3 implement processes for approving the bank's third-party providers, including the

third parties' financial condition, business resilience, and IT security posture;

1.2.4 escalate and report all information and cyber security incidents to the board, IT steering committee, government agencies, and law enforcement agencies, as appropriate;

1.2.5 identify, measure, monitor and mitigate information and cyber security risk;

1.2.6 coordinate and collaborate information and cyber security risk management activities with relevant internal and external stakeholders;

1.2.7 implement a cyber-security awareness program for all employees and the Board;

1.2.8 provide periodic reports (at a minimum quarterly) to the Board on the status of information and cyber security program;

1.2.9 share information regarding cyber threats and attacks with other banks and security agencies;

1.2.10 formulate recovery procedures for information and cyber risk incidents, minimise losses and ensuring operations return to normal;

1.2.11 ensure availability of officers with suitable qualifications and experience to manage cyber security risks;

1.2.12 report all information and cyber risk incidents to the Registrar immediately as and when they happen. A bank should also communicate with relevant internal and external stakeholders to ensure coordinated response to incidents;

1.2.13 ensure that staffing levels are adequate to handle present and expected work demands, and to cater reasonably for staff turnover;

1.2.14 ensure that an adequate training programme is in place for IT personnel and staff of IT-related functions in case of material skills gaps;

1.2.15 establish a clear IT organization structure and document and approve related job descriptions of individual IT functions;

1.2.16 Ensure proper segregation of duties within IT functions to ensure an effective IT control environment;

1.2.17 Implement adequate compensating controls where segregation of duties is not possible; and

1.2.18 Establish an IT planning or steering committee, which ensure effective use of IT resources.

1.3 Chief Information Security Officer

A bank shall have a Chief Information Security Officer or a similar designated officer responsible for information and cyber security of the bank, whose responsibilities shall be to-

1.3.1 implement the Cyber Security Risk Management Framework and associated policies;

1.3.2 ensure compliance with existing national ICT-related legislation, policies and regulations;

1.3.3 formulate procedures and processes for measuring and monitoring information and cyber security risks and implementing mitigation measures and controls;

1.3.4 ensure deployment of strong authentication measure to protect customer data, transactions and critical systems;

1.3.5 promote information and cyber security risk awareness and provide training on mitigating measures across the bank;

1.3.6 facilitate professional cyber security related trainings to improve technical proficiency of staff;

1.3.7 establish a cyber-security incident response program with clearly defined and documented roles and responsibilities of managing cyber-attacks and communication channels amongst relevant stakeholders;

1.3.8 ensure that regular and comprehensive information and cyber security risk assessments are conducted and adequate processes are in place for monitoring IT systems to detect cyber security events and incidents in a timely manner;

1.3.9 periodically test disaster recovery and business continuity plans to ensure that the bank can continue to function and meet its regulatory obligations in the event of a cyber-attack or incident; and

1.3.10 provide reports to the senior management on the overall status of the information cyber security programme.

1.4 Information and Cyber Security Risk Management

A bank shall have an information and cyber security risk control function which shall perform the following tasks-

1.4.1 identify, measure, monitor and mitigate information and cyber security risk in the second line of defence in risk governance;

1.4.2 support the board and senior management in developing and implementing the risk strategy;

1.4.3 monitor and ensure compliance with technical and operational Information and cyber security standards, policies and regulations for both internal and external stakeholders;

1.4.4 establish and document the Information and cyber security program that is consistent with the banks enterprise risk management framework;

1.4.5 ensure implementation of the Information and Cyber Security Risk Management Framework;

1.4.6 determine the bank's cyber risk tolerance and mitigation measures in line with business strategy;

1.4.7 draw up regular information and cyber risk reports for the board and senior management;

1.4.8 put in place an information and cyber risk inventory and draw up the overall risk profile of the institution;

1.4.9 coordinate information and cyber security awareness program for all employees; and

1.4.10 coordinate red team exercises and penetration testing;

1.5 Information Technology Audit

A bank shall:

1.5.1 establish an organizational structure and reporting lines for IT audit function in a way that preserves the independence and objectivity of the function;

1.5.2 ensure that the scope of IT audit is comprehensive and includes all critical IT operations and controls;

1.5.3 develop an IT audit plan, comprising auditable IT areas for the coming year,. The IT audit plan should be approved by the bank's Board Audit Committee;

1.5.4 establish an audit cycle that determines the frequency of IT audits commensurate with the criticality and risk of the IT system or process;

1.5.5 implement a follow-up process to track and monitor IT audit issues, as well as an escalation process to notify the relevant IT and business management of key IT audit issues; and

1.5.6 where necessary, engage external specialists or internal technology auditors of other entities of the same banking group to provide IT audit support.

1.6 IT Strategy

A bank shall have an IT Strategy which should be aligned with bank's overall business strategy and the Strategy shall define-

1.6.1 how IT should evolve to effectively support the bank's business strategy, including the evolution of the organisational structure, IT system changes and key dependencies with third parties;

1.6.2 the strategy and evolution of the reference architecture of IT, including third party dependencies;

1.6.3 clear information security objectives, focusing on IT systems and IT services, people and processes;

1.6.4 an acceptable level of detail, including measurable goals;

1.6.5 a set of action plans to support the IT strategy, which should be communicated to all relevant staff (including third party providers where applicable and relevant); and

1.6.6 processes to monitor and measure the effectiveness of the implementation of the IT strategy.

2. INFORMATION AND CYBER SECURITY RISK MANAGEMENT FRAMEWORK

2.1 A bank shall establish an information and cyber security risk management framework to manage information and cyber security risk in a systematic and consistent manner. The framework should include the following:

a) roles and responsibilities in managing information and cyber security risks;

b) risk tolerance;

c) methodology for the identification and classification of information and IT assets;

d) identification and measurement of impact and likelihood of current and emerging threats, risks and vulnerabilities;

e) risk mitigation through the implementation of effective controls and risk transfer practices;

f) periodic update and monitoring of identified risks and the effectiveness of controls to include changes in systems, environmental or operating conditions that would affect risk analysis;

g) timely and effective reporting processes on information security risks and the effectiveness of risk mitigation measures;

h) business resumption processes that provide guidance on how a bank should respond in order to contain, resume and recover from successful system disruptions and cyber-attacks;

i) ongoing Information and cyber security risk awareness programs;

j) processes to coordinate and collaborate with relevant internal and external stakeholders to strengthen cyber resilience;

k) methodology for allocation of an adequate IT budget based on a bank's structure and size of its information and cyber risk function; and

l) information and cyber security incident management plan that provides a roadmap for the actions the bank will take during and after a security incident.

2.2 A bank shall ensure that the information and cyber security risk management framework is documented, and updated with documented lessons learned during its implementation and monitoring.

2.3 The information and cyber security risk management framework should be approved and reviewed at least annually, by the board.

2.4 A bank should identify, establish and regularly update a mapping of the information assets supporting their business functions and supporting processes. Information assets that support critical business functions should be monitored.

2.5 A bank should classify the identified business functions, supporting processes and information assets in terms of criticality. To define the criticality of these identified business functions, supporting processes and information assets, a bank should, at a minimum, consider the confidentiality, integrity and availability requirements.

2.6 A bank shall ensure asset owners, who are accountable for the classification of the information assets, should be identified. The bank should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed, at least annually.

2.7 A bank shall ensure that it continuously monitors threats and vulnerabilities relevant to its business processes, supporting functions and information assets and must regularly review the risk scenarios impacting them.

2.8 A bank shall conduct IT risk assessments that includes impact analysis and consequences of these risks on the overall business and operations.

2.9 A bank shall maintain an up to date risk register, which facilitates the monitoring and reporting of information and cyber security risks. Risks of the highest severity should be monitored closely with regular reporting on the actions that have been taken to mitigate them.

3. MANAGEMENT OF IT OUTSOURCING RISKS

Where a bank intends to outsource or engage third party service providers for some of its IT related functions, the bank shall:

3.1 have a comprehensive policy to guide the assessment of whether and how those activities can be appropriately outsourced;

3.2 establish a comprehensive outsourcing risk management programme to address the outsourced activities and the relationship with the service provider;

3.3 carry out due diligence prior to engaging a service provider to determine its viability, capability, reliability, track record and financial position;

3.4 ensure that contractual terms and conditions governing the roles, relationships,

obligations and responsibilities of all contracting parties are set out fully in written agreements;

3.5 approve any significant sub-contracting of services and require that the original technology service provider to be responsible for its sub-contracted services;

3.6 ensure that the service provider grants access to all parties nominated by the bank to its systems, operations, documentation and facilities in order to carry out any review or assessment for regulatory, audit or compliance purposes;

3.7 require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, computer files, records, object programs and source codes;

3.8 monitor and review the security policies, procedures and controls of the service provider on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations and services provided by the service provider;

3.9 require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures;

3.10 commission a detailed assessment of the technology service provider's IT control environment when outsourcing critical technology services; and

3.11 Liaise with contractors and service providers to ensure that all activities are in line with the bank's information and cyber security policies and the business continuity plans.

Cloud Computing

A bank shall not outsource hosting of core banking systems and applications to third party cloud service providers. Where a bank intends to adopt cloud computing, the bank shall:

a) ensure a cloud computing policy is in place that covers cyber security risk;
b) operate its own cloud service or utilize group cloud infrastructure if the bank is part of a banking group;
c) conduct due diligence on the cloud service provider prior to being used by the bank for hosting of non-core banking systems and applications;
d) ensure that they have the ability to increase and decrease computing resources on demand without involving the service provider.
e) ensure that the contract with the service provider addresses significant issues such as financial and control audit, right to audit, ownership of data and programs and continuity service.

f) determine the extent of its authority to define control limitations and access to data for systems and applications using cloud;
g) ensure that all risks associated with outsourcing hosting of non-core banking applications to third party cloud service providers are adequately mitigated; and
h) ensure availability of a periodically tested business continuity plan for the cloud service;

4. ACQUISITION AND DEVELOPMENT OF INFORMATION SYSTEMS

A bank shall have the process of acquiring and/or developing information systems. The process should include planning, deploying, testing, maintaining, upgrading, and retiring information systems. Policies and procedures should be in place to govern the initiation, prioritization, approval, and control of IT projects. Progress reports of major IT projects should be submitted to and reviewed by the IT steering committee and the board periodically.

4.1 IT project management

A bank shall:

4.1.1 draw up a project management framework that includes quality assurance and risk management standards and procedures, critical success factors for each project phase, definition of project milestones and deliverables;

4.1.2 clearly document project plans for all IT projects that set out deliverables to be realised at each phase of the project as well as milestones to be reached;

4.1.3 ensure that user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation are approved by the relevant business and IT management;

4.1.4 establish management oversight of the project to ensure that milestones are reached and deliverables are realised in a timely manner; and

4.1.5 escalate issues or problems which could not be resolved at the project committee level to senior management for attention and intervention.

4.2 Security requirements and testing

A bank shall:

4.2.1 ensure that there is a high degree of integrity for all systems and data;

4.2.2 establish a methodology for system testing;

4.2.3 ensure that full regression testing is performed before system rectification or enhancement is implemented;

4.2.4 conduct penetration testing prior to the commissioning of a new system which offers Internet accessibility and open network interfaces. The bank should also perform vulnerability scanning of external and internal network components that support the

new system; and

4.2.5 maintain separate physical or logical environments for development, user acceptance testing (UAT) and production, and closely monitor vendor and developers' access to UAT environment.

4.3 Source code review

4.3.1 A bank shall rigorously test specific application modules and security safeguards with a combination of source code review, exception testing and compliance review to identify errant coding practices and systems vulnerabilities that could lead to security problems, violations and incidents.

4.4 End user development and Business Managed Applications

4.4.1 A bank shall perform an assessment to ascertain the importance of business application tools and software.

4.4.2 A bank shall ensure that information security controls and recovery measures of these business managed applications are aligned with the overall risk appetite of the institution and their criticality assessment.

4.4.3 A bank shall review and test end user developed program codes, scripts and macros before they are used in order to ensure the integrity and reliability of the applications.

5. IT SERVICE MANAGEMENT

A bank shall put in place a robust IT service management framework that comprise the governance structure, processes and procedures for change management, software release management, program migration, incident and problem management as well as capacity management.

5.1 Change management

A bank shall-

5.1.1 establish a change management process to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner;

5.1.2 ensure change management process applies to changes pertaining to system and security configurations, patches for hardware devices and software updates;

5.1.3 perform a risk and impact analysis of any change request in relation to existing infrastructure, network, up-stream and downstream systems;

5.1.4 adequately test the impending change and ensure that it is accepted by users prior to the migration of the changed modules to the production system. The bank should develop and document appropriate test plans for the impending change. The bank should obtain test results with user sign-offs prior to the migration;

5.1.5 ensure all changes to the production environment are approved by personnel delegated with the authority to approve change requests;

5.1.6 perform backups of affected systems or applications prior to the change;

5.1.7 establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. The bank should establish alternative recovery options to address situations where a change does not allow the bank to revert to a prior status; and

5.1.8 ensure that the audit and security logging facility is enabled to record activities that are performed during the migration process.

5.2 Program migration

Program migration involves the movement of software codes and scripts from the development environment to test and production environments. Unauthorised and malicious codes, which are injected during the migration process, could compromise data, systems and processes in the production environment.

A bank shall;

5.2.1 separate physical or logical environments for systems development production;

5.2.2 perform a risk assessment and ensure that sufficient preventive and detective controls have been implemented before connecting a non-production environment to the Internet;

5.2.3 enforce segregation of duties and/or controls for development, compilation and movement of object codes from one environment to another; and

5.2.4 replicate and migrate successful changes in the production environment to disaster recovery systems or applications for consistency.

5.3 Incident management

A bank shall-

5.3.1 appropriately manage incidents to avoid a situation of mishandling that result in a prolonged disruption of IT services or further aggravation;

5.3.2 establish an incident management framework with the objective of restoring normal IT service to a safe state, within defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) with minimal impact to the bank's business operations;

5.3.3 establish the roles and responsibilities of staff involved in the incident management process, which includes recording, analysing, remediating and monitoring incidents;

5.3.4 define and document appropriate incident severity levels as part of incident analysis and may delegate the function of determining and assigning the severity levels to a centralised technical helpdesk function;

5.3.5 establish corresponding escalation and resolution procedures where the resolution timeframe is commensurate with the severity level of the incident;

5.3.6 test the predetermined escalation and response plan for security incidents on a regular basis;

5.3.7 form an emergency response team, comprising staff within the bank with necessary technical and operational skills to handle major incidents;

5.3.8 ensure senior management is informed where major incidents further develop unfavourably into a crisis so that the decision to activate the disaster recovery plan can be made on a timely basis;

5.3.9 include in their incident response procedures a predetermined action plan to address public relations issues;

5.3.10 keep customers informed of incidents that may impact the customers and require their attention. The bank should also assess the effectiveness of the mode of communication, including informing the general public, where necessary;

5.3.11 perform a root-cause and impact analysis for major incidents which result in severe disruption of IT services and take corrective and preventive measures to prevent the recurrence of similar incidents;

5.3.12 ensure the root-cause and impact analysis report should cover the following areas:

a) Root Cause Analysis

i. Date of Incident occurrence;

ii. Location of incident;

iii. The cause and how the incident happened;

iv. Frequency of similar incident over the last 3 years; and

v. Lessons learnt from the incident

b) Impact Analysis

i. Extent, duration or scope of the incident including information on the systems, resources, customers that were affected;

ii. Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and

iii. Breach of regulatory requirements and conditions as a result of the incident.

c) Corrective and Preventive Measures

i. Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and/or compensation;

ii. Measures to address the root cause of the incident; and

iii. Measures to prevent similar or related incidents from occurring.

5.3.13 adequately address all incidents within corresponding resolution timeframes and

monitor all incidents to their resolution.

5.4 Problem management

5.4.1 A bank should establish clear roles and responsibilities of staff involved in the problem management process.

5.4.2 A bank should identify, classify, prioritise and address all problems in a timely manner.

5.4.3 Abank should clearly define criteria to categorise problems by severity level target resolution time for each severity level.

5.4.4 A bank should perform trend analysis of past incidents to facilitate the identification and prevention of similar problems.

5.5 Capacity management

5.5.1. The bank should implement performance and capacity planning and monitoring process to prevent, detect and respond to important performance issues of IT systems and IT capacity shortages in a timely manner.

5.5.2. The bank should establish monitoring processes and implement appropriate thresholds to provide sufficient time to plan and determine additional resources to meet operational and business requirements effectively.

6. BUSINESS CONTINUITY MANAGEMENT

A bank shall-

6.1 conduct a business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impact, quantitatively and qualitatively, using internal and/or external data and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes and information assets, and their interdependencies in accordance with the information security risk management process;

6.2 ensure that IT systems and IT services are designed and aligned with their BIA;

6.3 document Business Continuity Plans (BCPs) based on BIA and ensure the plans are approved by the board. Banks should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans;

6.4 ensure BCPs include RTOs and RPOs and prioritise business continuity actions using a risk-based approach;

6.5 include a range of different scenarios and describe how IT systems and services; and information security is ensured based on these scenarios;

6.6 develop response and recovery plans based on the BIA and plausible scenarios that specify conditions for activation of the plan and actions to be taken to ensure the availability, continuity and recovery of banks' critical IT systems and IT services;

6.7 ensure response and recovery plans consider both short-term and long-term recovery options and are documented and updated. The plans should focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies. The plans should also consider alternative options where recovery may not be feasible in the short term because of cost, risks, logistics, or unforeseen circumstances;

6.8 establish a recovery site that is geographically separate and has a different risk profile from the primary site to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site;

6.9 test their BCPs and ensure that the operation of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties) are tested at least annually;

6.10 document test results and any identified deficiencies resulting from the tests should be analysed, addressed and reported to senior management;

6.11 Ensure that the BCP should be updated based on test results, current threat intelligence

and lessons learnt from previous events;

6.12 involve business users in the design and execution of comprehensive test cases and the ability of staff to execute the necessary emergency and recovery procedures;

6.13 ensure that effective crisis communication measures are in place so that all relevant internal and external stakeholders are informed in a timely and appropriate manner;

6.14 define and implement data and IT systems backup and restoration procedures. The scope and frequency of backups should be set in line with business recovery requirements and the criticality of the data and the IT systems, assessed according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis; and

6.15 ensure that data and IT system backups are stored in one or more locations out of the primary site, which are secure and sufficiently remote from the primary site so as to avoid being exposed to the same risks.

7. MANAGEMENT OF OPERATIONAL INFRASTRUCTURE SECURITY

Protection of information security

A bank shall:

a) develop and document an information security policy which should define the high-level principles and rules to protect the confidentiality, integrity and availability of banks' and their customers' information;

b) establish and implement security measures to mitigate the ICT risks that they are exposed to.

c) develop a comprehensive data loss prevention strategy to protect sensitive or confidential information, taking into consideration the following specifications:

   i. Data at endpoint - Data which reside in notebooks, personal computers, portable storage devices and mobile devices;

   ii. Data in motion - Data that traverse a network or that is transported between sites; and

   iii. Data at rest - Data in computer storage, which includes files stored on servers, databases, backup media and storage platforms.

d) implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres. The bank should protect confidential information stored in all types of endpoint devices with strong encryption;

e) implement appropriate security measures including sending information through encrypted channels or encrypting the email and the contents using strong encryption with adequate key length based on criticality assessment;

f) encrypt and protect confidential information stored on IT systems, servers and databases through strong access controls, bearing in mind the principle of least privilege[1]; and

g) implement appropriate media sanitisation methods that take into consideration security requirements of the data residing on storage media to prevent the loss of confidential information through the disposal of IT systems.

[1] Least privilege principle refers to the assignment of privileges on a need-to-have basis.

7.1 Technology refresh management

A bank shall:

7.1.1 maintain an up-to-date inventory of software and hardware components used in the production and disaster recovery environments, which includes all relevant associated warranty and other support contracts related to the software and hardware components;

7.1.2 ensure that the IT asset inventory should be sufficiently detailed to enable the prompt identification of an IT asset, its location, security classification, and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks;

7.1.3 actively manage its IT systems and software so that outdated and unsupported systems, which significantly increase its exposure to security risks are replaced on a timely basis. The bank should pay close attention to the product's end-of-support ("EOS") date, as it is common for vendors to cease the provision of patches, including those relating to security vulnerabilities that are uncovered after the product's EOS date;

7.1.4 establish a technology refresh plan to ensure that systems and software are replaced in a timely manner. The bank should conduct a risk assessment for systems approaching EOS dates to assess the risks of continued usage and establish effective risk mitigation controls where necessary; and

7.1.5 monitor that the IT assets are supported by their vendors or in-house developers and that all relevant patches and upgrades are applied based on a documented process. The risks stemming from outdated or unsupported IT assets should be assessed and mitigated.

7.2 Networks and security configuration management

A bank shall-

7.2.1 configure IT systems and devices with security settings that are consistent with the expected level of protection. The bank should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment;

7.2.2 conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation. The frequency of enforcement reviews should be commensurate with the risk level of systems;

7.2.3 deploy and update anti-virus software to servers and workstations; and

7.2.4 install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical points of its IT infrastructure to protect the network perimeters.

7.3 Vulnerability assessment and penetration testing

A bank shall-

7.3.1 conduct vulnerability assessments (VAs) regularly to detect security vulnerabilities in the IT environment;

7.3.2 establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed; and

7.3.3 carry out penetration tests to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system at least annually.

7.4 Patch management

7.4.1 A bank shall establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches.

7.4.2 A bank shall establish the implementation timeframe for each category of security patches to deploy security patches in a timely manner.

7.4.3 A bank shall perform rigorous testing of security patches before deployment into the production environment.

7.5 Security monitoring

The bank shall-

7.5.1 establish appropriate security monitoring systems and processes to facilitate prompt detection of unauthorised or malicious activities by internal and external parties;

7.5.2 implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the bank against network intrusion attacks as well as provide alerts when an intrusion occurs;

7.5.3 Implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the

identification of unauthorised changes;

7.5.4 regularly review security logs of systems, applications and network devices for anomalies;

7.5.5 adequately protect and retain system logs in line with statutory requirements to facilitate document retention and protection;

7.5.6 grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. The bank should ensure that the resource owner duly authorises and approves all requests to access IT resources;

7.5.7 subject employees of vendors or service providers that have access to bank systems to close supervision, monitoring and access restrictions similar to those expected of its own staff;

7.5.8 Ensure that records of user access are uniquely identified and logged for audit and review purposes;

7.5.9 perform regular reviews of user access privileges to verify that privileges are granted appropriately and according to the 'least privilege' principle. The process should facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access; and

7.5.10 enforce strong password controls over users' access to applications and systems.

7.6 Privileged access management

7.6.1 A bank should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.

7.6.2 A bank should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed. The bank should adopt the following controls and security practices:

a) Implement strong authentication mechanisms;

b) Institute strong controls over remote access by privileged users;

c) Restrict the number of privileged users;

d) Grant privileged access on a need-to-have basis;

e) Maintain audit logging of system activities performed by privileged users;

f) Disallow privileged users from accessing systems logs in which their

activities are being captured;

g) Review privileged users' activities on a timely basis;

h) Prohibit sharing of privileged accounts; and

i) Protect backup data from unauthorised access.

7.7 Data Center (Threat and vulnerability risk assessment, Security, Resilience)

A bank shall-

7.7.1 regularly conduct Threat and Vulnerability Risk Assessment (TVRA) based on various possible scenarios of threats, which include theft, explosives, arson, unauthorised entry, external attacks and insider sabotage;

7.7.2 include the scope of the TVRA a review of the Data Center's (DC) perimeter and surrounding environment, as well as the building and DC facility;

7.7.3 limit access to DC to authorised staff only and grant access to the DC on a need to have basis;

7.7.4 ensure proper notification and approval of non-DC personnel such as vendors, system administrators or engineers and ensure that visitors are accompanied at all times by an authorised employee while in the DC;

7.7.5 ensure that the perimeter of the DC, DC building, facility, and equipment room are physically secured and monitored;

7.7.6 assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications;

7.7.7 rigorously control and regulate the environment within a DC. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical in ensuring uptime and system reliability; and

7.7.8 implement fire protection and suppression; and sufficient backup power in the DC.

8. E-BANKING[2]

8.1 E-banking systems security

A bank shall-

8.1.1 evaluate security requirements associated with its e-banking services and adopt effective encryption algorithms that are in line with international standards and best practices;

8.1.2 ensure that there is adequate protection of sensitive or confidential information used for mobile online services and payments;

8.1.3 implement controls to ensure that e-banking information processed, stored or transmitted between the bank and its customers is accurate, reliable and complete;

8.1.4 implement monitoring or surveillance systems so that it is alerted of any abnormal system activities, transmission errors or unusual online transactions. The bank should establish a follow-up process to verify that these issues or errors are adequately addressed subsequently;

8.1.5 maintain high resiliency and availability of its e-banking services and supporting systems. The bank should put in place measures to plan and track capacity utilisation as well as guard against online attacks;

8.1.6 implement strong authentication at login for Internet banking financial systems and transaction-signing for authorising transactions;

8.2 Customer security

A bank shall-

8.2.1 perform adequate identity checks when any customer requests a change to account information or contact details that are used to receive important information. The bank should also monitor the activities of the customer's accounts concerned;

8.2.2 warn customers of the customers' obligations to take reasonable security precautions to protect the devices they use in e-banking and keep the passwords they use for accessing e-banking secure and secret;

8.2.3 adequately manage the risk associated with fraudulent websites, phishing emails or similar scams which are designed to trick their customers into revealing sensitive

[2] E-banking refers to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or Internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices.

information;

8.2.4 ensure that sufficient guidance and training are given to officers who handle customers' enquiries related to the security precautions of e-banking;

8.2.5 facilitate customers' timely detection of unauthorized transactions that may arise as a result of fraudulent activities related to e-banking channels; ,

8.2.6 establish effective channels to notify customers once they initiate transactions of higher risk;

8.2.7 send timely notifications for all card-not-present (CNP) transactions;

8.2.8 use a risk-based approach to follow up situations where notifications that cannot be delivered to the customers concerned; and

8.2.9 ensure that unless a customer acts fraudulently or with gross negligence, he or she should not be responsible for any direct loss suffered by him or her as a result of unauthorized transactions in relation to the use of e-banking services.

8.3 Payment card security (Automated Teller Machines, credit and debit cards)

A bank shall-

8.3.1 implement adequate safeguards to protect sensitive payment card data and ensure that data is encrypted to promote confidentiality and integrity of data in storage and transmission;

8.3.2 deploy secure chips to store sensitive payment card data;

8.3.3 only allow online transaction authorisation for transactions performed with ATM cards;

8.3.4 restrict authentication of customers' sensitive static information to the card issuer, and not a third party payment processing service provider;

8.3.5 promptly notify cardholders via transaction alerts when withdrawals/charges exceeding customer-defined thresholds are made on the customers' payment cards;

8.3.6 implement robust fraud detection systems with behavioural scoring or equivalent, and correlation capabilities to identify and curb fraudulent activities. The bank should set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities;

8.3.7 follow up and investigate on transactions exhibiting behaviour that deviates

significantly from a cardholder's usual card usage patterns;

8.3.8 consider putting in place the following measures to counteract fraudsters' attacks to secure consumer confidence using ATMs:

a) install anti-skimming solutions to detect the presence of foreign devices placed over or near a card entry slot;

b) install detection mechanisms and send alerts to appropriate staff at the bank for follow-up response and action;

c) implement appropriate measures to prevent shoulder surfing of customers' PINs; and

d) conduct video surveillance of activities at these machines, and maintain the quality of CCTV footage.