SUPERVISORY AND REGULATORY GUIDELINES: 2003-03
Technology Risk
Issued: 15th January 2016

TECHNOLOGY RISK MANAGEMENT GUIDELINES

1. INTRODUCTION

1.1 The Central Bank of The Bahamas *("the Central Bank")* is responsible for the licensing, regulation and supervision of banks and trust companies operating in and from within The Bahamas pursuant to the Banks and Trust Companies Regulation Act, 2000 (Chapter 316) and the Central Bank of The Bahamas Act, 2000 (Chapter 351). Additionally, the Central Bank has the duty, in collaboration with licensees, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

1.2 All licensees are expected to adhere to the Central Bank's licensing and prudential requirements, on-going supervisory programmes, including periodic on-site examinations and required regulatory reporting. Licensees are further expected to conduct their affairs in conformity with all other Bahamian legal requirements.

1.3 Advancements in technology have allowed great opportunities for licensees to provide new banking models, services and products. Social media, internet banking and mobile technology all have helped to revolutionize how financial transactions are executed and supported. However, with this evolution of enhanced services, the financial sector is also introduced to sophisticated and complex sets of vulnerabilities and security issues. Assets that were once physically protected are accessible online; services/delivery/distribution channels are vulnerable to disruption (intentional and unintentional) and criminals have new opportunities for theft and fraud. Exploitation of weaknesses in such technologies can lead to theft of intellectual property and other sensitive economic information. Such losses can have a negative impact on an organization's reputation and bottom line, as well as incurring fines for regulatory violations.

1.4 The aim of these Guidelines is to highlight risks inherent to deployment and management of technology as well as to provide broad guidance for licensees on risk management principles and security practices which may assist the financial sector with:

1.4.1 Establishing a sound and robust technology risk management framework;

1.4.2 Strengthening system security, reliability, availability and recoverability; and

1.4.3 Emphasizing the benefit of using appropriate technologies and control mechanisms that protect customer data and transactions.

2. EXECUTIVE SUMMARY

2.1 Technology risk is a subset of operational risk that can significantly impact the overall success of a licensee. Risks left unaddressed could significantly impact the confidentiality, integrity and system availability of a licensee's data. The following guidance establishes supervisory expectations relative to management of technology risks by licensees.

3. APPLICABILITY

3.1 These Guidelines apply, as appropriate, to all licensees.

4. SUPERVISORY APPROACH

4.1 The Central Bank aims to provide licensees general guidance for addressing risks associated with managing technology used in business operations, but which is not intended to be a prescriptive and comprehensive approach for managing all technology risks. The objective of the Guidelines is to promote the adoption of sound practices and processes for managing technology risks.

4.2 The Central Bank is not seeking to replace or endorse existing industry standards and guidelines. However, useful guidance is expected be obtained from industry generally accepted standards such as COBIT[1], ISO standards[2], ITIL[3] and other guidelines published by the Central Bank. Licensees should apply such guidance in a manner commensurate with the risk profile of the licensee.

4.3 All licensees are expected to apply a risk management framework that is commensurate with the licensees risk profile.

IT RISKS

5. TECHNOLOGY RISKS

5.1 Technology Risks are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity or failure arising from the use of or reliance on computer hardware, software, electronic devices, online networks, and

[1] COBIT 5: Formerly known as Control Objectives for Information and related Technology (COBIT); now used only as the acronym in its fifth iteration. A complete, internationally accepted framework for governing and managing enterprise information and technology (IT) that supports enterprise executives and management in their definition and achievement of business goals and related IT goals. COBIT describes five principles and seven enablers that support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices. Source *ISACA*' Glossary, *http://www.isaca.org/Pages/Glossary.aspx?tid=1207&char=C*

[2] ISO: International Organization for Standardization (ISO); *Source* ISACA' Glossary, http://www.isaca.org/Pages/Glossary.aspx?tid=1526&char=I

[3] ITIL: The UK Office of Government Commerce (OGC) IT Infrastructure Library. A set of guides on the management and provision of operational IT services. Source ISACA' Glossary, http://www.isaca.org/Pages/Glossary.aspx?tid=1546&char=I

telecommunications systems. These risks can also be associated with systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions and inadequate recovery capabilities.

5.2 IT risk encompasses the risk of loss resulting from inadequate or failed internal processes, people, systems, or external events impacting IT assets. IT assets include assets that are managed, developed or supported by a technology function, service providers or teams/individuals located within business units.

5.3 Given that IT risk is a subset of overall operational risk, a significant compromise in technology could impact an organization's ability to meet overall business objectives (including regulatory and prudential). IT security risks, which are a component of IT risks, arise when there is a compromise of:

5.3.1 Confidentiality – where there is unauthorized access to data and systems;

5.3.2 Integrity – where there is compromise to the completeness, accuracy and unauthorized changes to data and systems; or

5.3.3 Availability – where there is disruption to the accessibility to or usability of data and/or systems.

5.4 Breaches in technology could have significant consequences to licensees including reputational damage, regulatory breaches, and revenue and business losses.

IT GOVERNANCE

6. OVERARCHING APPROACH TO IT RISK MANAGEMENT

6.1 To mitigate and control technology risks, licensees may adopt a set of high level IT security principles that establish the foundation of the IT security risk management framework. Such principles should be integrated into a licensee's overall technology risk management framework.

6.2 This overarching framework typically will include established functions with clear roles and responsibilities, policies, standards, guidelines and procedures. It also collectively addresses technology, security, reputational and operational risks for the licensee.

7. BOARD OF DIRECTORS AND SENIOR MANAGEMENT

7.1 Given the importance of the technology function to licensees, the Board and Senior Management should have oversight over technology risks to ensure that the organization's IT functions are aligned with and capable of supporting the licensee's business strategies and objectives.

Board of Directors and Senior Management – Roles and Responsibilities

7.2 The Board and Senior Management should ensure:

7.1.1 The IT strategy is aligned with the overall business strategy;

7.1.2 The establishment and ongoing maintenance of a robust technology risk management framework;

7.1.3 Its involvement in key IT decisions;

7.1.4 Effective internal controls and risk management practices are implemented to achieve ongoing security, reliability, resiliency and recoverability;

7.1.5 Adequate assessment of cost-benefit analysis of the technology investment; inclusive of reputation, customer confidence, consequential impact and legal implications, with regard to investment in controls and security measures for computer systems, networks, and data centers (DC), operations and backup facilities;

7.1.6 The establishment of technology policies, standards and procedures that govern the management of technology risks and safeguard the licensee's information system assets;

7.1.7 Regular review and updating of policies, standards and procedures to ensure documents remain relevant to current threats and technologies;

7.1.8 Implementation and execution of compliance processes to verify that IT security standards and procedures are enforced. Follow-up processes should be implemented so that compliance deviations are addressed and corrected on a timely basis;

7.1.9 Implementation of a screening process that is comprehensive and effective to assure careful selection of staff, vendors and contractors who support technology functions and to minimize technology risks due to system failure, internal sabotage or fraud;

7.1.10 That staff, vendors and contractors, who are authorized to access licensee systems, are formally required to protect sensitive or confidential information;

7.1.11 The establishment of a comprehensive IT security awareness training program to enhance the overall IT and IT security awareness level in the organization. The training program should include information on IT security policies and standards as well as individual responsibility in respect of IT security and measures that should be taken to safeguard information system assets. Every staff in the organization should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources;

7.1.12 Implementation of a training program that ensures training is conducted and updated at least annually. Training should also be extended to all new and existing staff, contractors and vendors who have access to licensee's IT resources and systems; and

7.1.13 The training program is endorsed by Senior Management. It should be reviewed and updated to ensure that the contents of the program remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks.

8. TECHNOLOGY RISK MANAGEMENT FRAMEWORK

8.1 The licensee's technology risk management framework should be established to manage technology risks in an efficient, effective and consistent manner. Framework attributes to consider include, but not limited to the following:

8.1.1 Clear roles and responsibilities in managing technology risks;

8.1.2 Identification and prioritization of information system assets;

8.1.3 Identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities;

8.1.4 Implementation and monitoring of appropriate practices and controls to mitigate risks; and

8.1.5 Periodic update and monitoring of risk assessments to include changes in systems, environmental or operating conditions that could affect risk analysis.

8.2 An effective risk management framework identifies the information systems assets that requires protection; identifies the direct and indirect threats in the IT environment; assesses the probability and potential impact of identified risks; for each risk identified evaluates, prioritizes and implements appropriate risk reduction controls; and facilitates the maintenance and reporting of valuable risk metrics that are periodically provided to the appropriate levels of management.

8.3 The following are key components of effective risk management:

Risk Identification

Risk identification involves:

8.3.1 Identification and criticality classification of information systems. A clear policy should be in place to detail the level of protection required based on the risk and criticality rating of the information system;

8.3.2 Identification and assessment of threats to the IT environment. Threats represent vulnerabilities to the IT environment identified in a licensee's internal and external networks, hardware, software, applications, systems interfaces, operations and human elements;

8.3.3 Consideration of all sources of threats in the risk analysis. Threat sources may be natural, human or environmental;

8.3.4 Vigilant monitoring of emerging security risks such as denial of service attacks, internal sabotage and malware infestation; and

8.3.5 Maintenance of an inventory of risks and controls applicable to the licensee.

Risk Assessment

8.4 Risk assessment involves:

8.4.1 Assessment and quantification of risk exposure and impact of such exposures to licensee's overall business and operations should an adverse event occur;

8.4.2 A process to report on and prioritize threats;

8.4.3 Risk mitigation and control strategies that are in alignment with the value of the licensee's information assets and organizational risk appetite;

8.4.4 A risk based approach that addresses risks based on probability and impact in the event a significant risk materializes. The costs associated with managing a licensee's identified risks should be balanced against the benefits derived while maintaining operational and financial stability;

8.4.5 Consideration for securing insurance against various risks including recovery and restitution; and

8.4.6 Specific assessment of threats to continuity of operations due to internally managed and outsourced functions.

Risk Monitoring and Reporting

8.5 Risk monitoring and reporting involves:

8.5.1 Risk monitoring and reporting to Senior Management and the Board. Regular reporting of significant risks and associated status of risk mitigation activities should be in place. Risks reported should be updated on an ongoing basis to ensure current threats and control activities are being communicated to Senior Management and the Board.

8.5.2 IT risks metrics to highlight systems, processes or infrastructure that have the highest risk exposure. An overall technology risk profile of the organization should also be provided to the Board and Senior Management. In determining the IT risk metrics, licensees should consider risk events, regulatory requirements and audit observations.

8.5.3 Periodic review and update of risk management processes, re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes.

Risk Mitigation and Control Activities Implementation

8.6 Risk Mitigation and Control Activities Implementation:

8.6.1 Ongoing application and management of control activities to mitigate identified risks;

8.6.2 Implementation, periodic refresh, communication and execution of procedures and activities to manage technology related risks; and

8.6.3 A risk acceptance strategy that involves accepting risk when it is presumed that the cost, effort or time required to address the risk is not feasible to pursue. The appropriate strategy is implemented based on management's risk appetite.

IT CONTROLS

9. MANAGEMENT OF IT OUTSOURCING RISKS[4]

9.1 As licensees strive to effectively achieve organizational goals, outsourcing has become more prevalent. As it has become more common to outsource, it is expected that the responsibility and accountability for the outsourced function or process, remains with the licensee. Outsourcing of technology services and functions can also change a licensee's risk profile.

9.2 Prior to the appointment of a service provider, due diligence should be carried out to determine its viability, capability, reliability, track record and financial position. This facilitates the Board of Directors and Senior Management understanding of risks associated with IT outsourcing.

9.3 Contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties should be set out fully in written agreements. The requirements and conditions covered in the agreements generally include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

9.4 The contractual agreements with the service provider should recognize the authority of regulators or their authorized agent to perform an assessment on the service provider's control environment relative to the service being performed.

9.5 Licensees should require the service provider to have or implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

9.6 Licensees should 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.

[4] Supervisory guidance relating to outsourcing is provided in the Central Bank's ***Guidelines on Minimum Standards for the Outsourcing of Material Functions***.

9.7 The outsourcing agreement should require the service provider to have or 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.

9.8 The provider's disaster recovery plan should be reviewed, updated and tested periodically to reflect changes in technology and operational requirements. The plan should take into account worse case disruption scenarios, unavailability of existing service provider, and should identify viable alternatives for resuming IT services. Licensees should ensure that the plan is shared with relevant stakeholders who are sufficiently trained on the recovery plan execution steps.

9.9 The Licensee should ensure that there is an exit strategy in place in the event of termination of the relationship.

10. SYSTEM DEVELOPMENT AND ACQUISITION (SDLC)

10.1 SDLC (System Development Life Cycle) refers to the phases deployed in the development or acquisition of a software system. SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and post-implementation review, but not the service delivery or benefits realization activities.[5]

10.2 There are inherent risks related to the development and deployment of technology. These include cost, business fit and compatibility, user proficiency, security of information, availability of systems during changes and involvement of business users for proper acceptance of the system. When deploying new systems, licensees should evaluate whether there are any deficiencies and defects at the system design, development and testing phases. Effective oversight should occur over the entire SDLC process.

10.3 The following should be considered by the licensee:

10.3.1 The licensee should establish an IT Steering Committee, consisting of business owners, the development team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

10.3.2 The licensee should employ technology management best practices such as:

[5] *ISACA*, Glossary, *http://www.isaca.org/Pages/Glossary.aspx?tid=1897&char=S*

a) Clear definition of the roles and responsibilities of staff involved in the project;

b) Ensure tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables;

c) Utilize project plans for all IT projects. Such plans should identify what deliverable is expected and what milestone should be accomplished at each phase of the project;

d) Ensure 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; and

e) Ensure there is project management oversight monitoring that milestones are reached and deliverables are realized on a timely basis inclusive of an escalation process to senior management for issues that require attention and intervention.

10.3.3 The licensee should integrate and manage security requirements throughout the project lifecycle. These include the following project security best practices:

a) Ensure clear specification of security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling is in place; and also a compliance check of the licensee’s security standards against the relevant statutory requirements;

b) Ensure system testing methodology is in place. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions;

c) Ensure full regression testing is performed before system changes or enhancement is implemented;

d) Review and sign off on the outcome of the changes by users whose systems and operations are affected by the change being implemented;

e) Conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces due to the increased risks associated with such services;

f) Perform vulnerability scanning of external and internal network components that support new systems; and

g) Maintain separate physical or logical environments for unit, integration, as well as system and user acceptance testing (UAT).

Additionally, vendor and developers’ access to UAT environments should be closely monitored.

10.3.4 Introduction of new functionality and modules to the existing technology environment may require customizations of the system before such features may be properly adapted in the environment.

10.3.5 Source code deployed to support associated technology should be reviewed as source code weaknesses may lead to intentional or unintentional manipulation of a vulnerability by an attacker.

10.3.6 Source code review is recommended to address such concerns. The review involves a methodical examination of the source code of an application with the objective of finding defects that are due to coding errors, poor coding practices or malicious attempts.

10.3.7 Source code reviews are designed to identify security vulnerabilities and deficiencies, and mistakes in system design or functionality relating to areas such as control structure, security, input validation, error handling, file update, function parameter verification, before the system is implemented. The following are considerations when evaluating sufficiency of source code deployed:

a) Confirm that systems have appropriate security controls, based on the type and complexity of services the systems provide;

b) Conduct a risk analysis of the system and based on the results customize tests that rigorously test specific application modules and security safeguards; and

c) A combination of source code review, exception testing and compliance reviews should be employed to identify poor coding practices and systems vulnerabilities that could lead to security problems, violations and incidents.

10.3.8 There should be adequate business recovery and back out plans in place should there be an unsuccessful deployment or significant issue that requires a roll back of the deployment.

10.3.9 There are common business application tools and software which allow business users to develop simple applications to automate their operations, perform data analysis and generate reports for the licensee and customers. Such end user tools should be subjected to a baseline level of controls similar to that of standard applications. Commensurate with the risk of the applicable end user tools the following is recommended:

a) Perform an assessment to ascertain the importance of these applications to the business;

b) Implement recovery measures, restriction of user access and data protection controls over such applications; and

c) Review and test end user developed program codes, scripts and macros before they are used so as to ensure the integrity and reliability of the applications. This include change and version management controls.

I*T SERVICE MANAGEMENT AND TECHNICAL OPERATIONS*

11. IT SERVICE MANAGEMENT

11.1 IT service management framework involves supporting IT systems, services and operations, change management, incident and problem management as well as ensuring the stability of the production IT environment.

11.2 A control framework around IT Service Management should comprise of the governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management. It is expected that:

11.2.1 Change management processes are in place to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner;

11.2.2 Change management processes should apply to changes pertaining to system and security configurations, patches for hardware devices and software updates;

11.2.3 Prior to deploying changes to the production environment, risk and impact analyses are performed of the change request in relation to existing infrastructure, network, up-stream and downstream systems. Assessments are also made to determine if the introduced change could lead to security implications or software compatibility problems to affected systems or applications;

11.2.4 Appropriate test plans are developed and documented to vet the impending change. Adequate testing is performed for any changes and such changes are accepted by users prior to the migration of the change to the production system. Test results with user sign-offs should be maintained prior to the migration of the change to production;

11.2.5 All changes to the production environment should be approved by personnel delegated with the authority to approve change requests;

11.2.6 To minimize risks associated with changes, backups should be performed for affected systems or applications prior to the change. Rollback plans should be in place to revert to a former version of the system or application should a problem be encountered during or after the deployment. Alternative recovery options should be established to address situations where a change does not allow the licensee to revert to a prior system status; and

11.2.7 Audit and security logs are enabled to record activities that are performed during the migration process. This information may be useful to facilitate investigations and troubleshoot issues, if required.

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

11.4 To prevent intentional and unintentional negative outcomes during the migration process, the following best practices are recommended:

11.4.1 Separate physical or logical environments for systems development, testing, staging and production should be established;

11.4.2 Where controls in the non-production environment are different or less stringent from those in the production environment, the licensee should perform a risk assessment and ensure that sufficient preventive and detective controls have been implemented before connecting a non-production environment to the internet;

11.4.3 Ensure proper segregation of duties is enforced so that no single individual has the ability to develop, compile and move object codes from one environment to another; and

11.4.4 After a change has been successfully implemented in the production environment, the change should also be replicated and migrated to disaster recovery systems or applications for consistency.

11.5 An IT incident occurs when there is an unexpected disruption to the standard delivery of IT services. The licensee should appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of IT services or further aggravation. Sound *incident management* practices include:

11.5.1 An incident management framework with the objective of restoring normal IT service as quickly as possible following an incident, and with minimal impact to business operations;

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

11.5.3 Assignment of incidents and management based on an appropriate severity level. As a part of incident analysis, a centralized technical helpdesk function, may determine and assign the relevant incident severity rating. The helpdesk staff should be sufficiently trained to discern incidents of high severity level;

11.5.4 Establishment and documentation of criteria used for assessing severity levels of incidents;

11.5.5 Establishment of escalation and resolution procedures. Resolution timeframes should be commensurate with the assigned severity level of the incident;

11.5.6 The established escalation and response plan for security incidents should be tested on a regular basis;

11.5.7 Existence of a computer emergency response team, comprising resources (internal and external) with necessary technical and operational skills to handle major incidents;

11.5.8 In the event that an incident becomes a crisis the following should be in place:

a) Sufficient and timely communication to Senior Management regarding the development of an incident so that a decision to activate the disaster recovery plan can be made on a timely basis; and

b) Procedures to communicate with the Central Bank in the event that a critical system has failed over to the disaster recovery system.

11.5.9 Incident response procedures should include a predetermined action plan to address public relations issues in order to maintain customer confidence throughout a crisis or an emergency situation. The licensee should assess the effectiveness of the mode of communication, including informing the general public, where necessary;

11.5.10 Performance of root-cause and impact analysis for major incidents which result in severe disruption;

11.5.11 Remediation actions are taken as necessary and the issue is monitored to closure to prevent the recurrence of similar incidents. Progress against remediation plans should be reported periodically to senior management until the remediation is complete;

11.5.12 Incident reports should include an executive summary of the incident, an analysis of the root cause which triggered the event, its subsequent impact as well as measures taken to address the root cause and consequences of the event;

11.5.13 The root-cause and impact analysis report should cover the following areas:

a) Root Cause Analysis

- When did it happen?
- Where did it happen?
- Why and how did the incident happen?
- How often had a similar incident occurred over the last 3 years?
- What lessons were learnt from this incident?

b) Impact Analysis

- Extent, duration or scope of the incident including information on the systems, resources, customers that were affected;
- Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and
- Breach of regulatory requirements and conditions as a result of the incident.

c) Corrective and Preventive Measures

- Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and/or compensation;
- Measures to address the root cause of the incident; and
- Measures to prevent similar or related incidents from occurring.

12. PROBLEM MANAGEMENT

12.1 The aim of ***problem management*** is to determine and eliminate an incident root cause to prevent the occurrence of repeated problems. Sound practices for problem management include:

12.1.1 Clearly established roles and responsibilities for staff involved in the problem management process;

12.1.2 Process in place to identify, classify, prioritize and address all problems in a timely manner;

12.1.3 Clear definition of the criteria used to categorize problems by severity level;

12.1.4 Effective monitoring and escalation of problems, target resolution times and establishment of appropriate escalation processes for each problem severity level; and

12.1.5 Performance of trend analysis of past incidents to facilitate the identification and prevention of similar or repeat problems.

13. CAPACITY AND PERFORMANCE MANAGEMENT

13.1 To ensure that IT systems and infrastructure are able to support business functions, licensees should ensure that indicators such as performance, capacity and utilization are monitored and reviewed. Sound ***capacity and performance management*** practices include:

13.1.1 Clearly established roles and responsibilities for staff involved in the capacity and performance management process;

13.1.2 Establishment of appropriate thresholds and performance metrics that enable monitoring of system performance and associated reporting of such metrics; and

13.1.3 Establishment of monitoring processes and implementation of appropriate thresholds to provide sufficient time to plan and determine additional resources required to meet operational and business requirements effectively.

14. SYSTEM RELIABILITY, AVAILABILITY AND RECOVERABILITY[6]

14.1 The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in a licensee's operational and functional capabilities. When critical systems fail, the disruptive impact on a licensee's operations or customers will usually be severe and widespread and could lead to serious consequences to the licensee's reputation. Examples of such events are system faults, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary data center.

14.2 Key points specific to technology include:

14.2.1 Assessing and defining the recovery requirements for each system used to support operations and processes;

14.2.2 Documenting contingency plans, taking into consideration varying scenarios of disruption (major and minor disruptions) including unavailability of peer or interdependent systems, supporting network and infrastructure, vendors and services providers, human resources and access to physical premises;

14.2.3 Where feasible licensees should develop built-in redundancies to reduce single points of failures;

14.2.4 Maintaining secondary hardware, software and network components to support a fast recovery;

14.2.5 Periodic evaluation of the recovery plan and incident response process should occur at least annually. During the review it should confirm that changes to business operations, systems and networks have been considered and where applicable included in the recovery plan and tests;

14.2.6 Licensees should define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for IT systems and applications. RTO is the duration of time, from the point of disruption, within which a system should be restored. RPO refers to the acceptable amount of data loss for an IT system should a disaster occur;

[6] Supervisory guidance relating to business continuity is provided in the Central Bank's ***Business Continuity Guidelines***.

14.2.7 Recovery sites should be geographically separate from the primary site to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site;

14.2.8 There are various considerations that determine the speed at which recovery is achieved. These include the criticality associated with resuming business operations, the type of services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers. Licensees may wish to explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance its recovery capability; and

14.2.9 The resiliency and robustness of critical systems that are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links. To minimize impact on business operations in the event of a disruption (e.g. due to hurricane), the licensee should ensure that there is cross-border network redundancy, with strategies such as engagement of different network service providers and alternate network paths, are instituted.

Disaster Recovery Testing

14.3 To ensure readiness during outages, licensees should take steps to validate the completeness and adequacy of recovery plans. To accomplish this, licensees should:

14.3.1 Test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures;

14.3.2 Ensure that disaster recovery tests cover various test scenarios, including total shutdown or incapacitation of the primary site as well as component failure at the individual system or application cluster level;

14.3.3 Test the recovery dependencies between systems and service providers (including those systems which are located offshore); and

14.3.4 Testing should involve business users in the design and execution of comprehensive test cases to verify that recovered systems function properly.

15. DATA BACKUP MANAGEMENT

15.1 An important part of system resumption is the restoration of data. To ensure that this process happens efficiently licensees should:

15.1.1 Develop a data backup strategy for the storage of critical information;

15.1.2 Consider the implementation of specific data storage architectures such as Direct-Attached Storage (DAS), Network-Attached Storage (NAS) or Storage Area Network (SAN) sub-systems connected to production servers. In this regard, processes should be in place to review the architecture and connectivity of sub disk storage systems for single points of failure and fragility in functional design and specifications, as well as the technical support by service providers;

15.1.3 Carry out periodic testing and validation of the recovery capability of backup media and assess if the backup media is adequate and sufficiently effective to support the recovery process; and

15.1.4 Encrypt backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.

16. OPERATIONAL INFRASTRUCTURE SECURITY MANAGEMENT

16.1 Measures should be taken to protect sensitive or confidential information such as customer personal, account and transaction data which are stored and processed in licensee systems.

16.2 Customers should be properly authenticated before access to online transaction functions and, sensitive personal or account information is permitted. Sensitive customer information including login credentials, passwords and personal identification numbers (PINs) should be secured against exploits such as account takeovers, ATM skimming, card cloning, hacking, phishing and malware.

16.3 To address internal and external threats that can lead to data loss, the following measures may be employed:

16.3.1 Licensees should identify important data and adopt adequate measures to detect and prevent unauthorized access, copying or transmission of confidential information;

16.3.2 Licensees should ensure protection of sensitive and confidential information at all points along the flow of data. This includes data at endpoint (such as end user devices – mobile, notebooks, personal computers, and removable media), data in transit (data flowing in networks or between sites) and data at rest (data stored in databases, servers, on backup media and in storage platforms);

16.3.3 Endpoint devices should protect confidential information stored on the devices with strong encryption. There should also be appropriate controls to address the risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centers;

16.3.4 It is not recommended for licenses to use unsafe internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information. Appropriate control measures should be in place to prevent and detect the use of such services within the licensee or to report issues with such services should they be employed;

16.3.5 Whenever confidential data is exchanged internally or externally, appropriate measures should be taken to send information via encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length. The encryption key should be sent via a separate transmission channel to the intended recipients. Alternatively, licensees may choose other secure means to exchange confidential information with its intended recipients;

16.3.6 Confidential information stored on IT systems, servers and databases should be encrypted and protected through strong access controls, and restricting access on a least privilege basis; and

16.3.7 The licensee should assess various methods by which data could be securely removed from storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems. In determining the appropriate media sanitization method to use, consideration should be given to security requirements of the data residing on the media.

17. DATA CENTER PROTECTION AND CONTROLS

17.1 Typically a licensee’s critical systems and data are concentrated and maintained in a data center (DC). It is therefore important that the DC is resilient and physically secured from internal and external threats.

17.2 Appropriate controls expected for data center protection include performance of a Threat and Vulnerability Risk Assessment (TVRA) to identify security threats to and operational weaknesses in a DC in order to determine the level and type of protection that should be established to safeguard it.

17.3 The assessment should take into account numerous factors such as criticality of the DC, geographical location, multi-tenancy and type of tenants occupying the DC, impact from natural disasters, and the political and economic climate of the country in which the DC resides. Various possible scenarios of threats which include theft, explosives, arson, unauthorized entry, external attacks and insider sabotage.

17.4 It is recommended that the licensee’s TVRA review scope include a review of the DC’s perimeter and surrounding environment, as well as the building and DC facility. A review of daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls is also deemed beneficial.

17.5 When selecting a DC provider, licensees should obtain and assess the TVRA report on the DC facility. It should be confirmed that the reports are current and that the DC provider is committed to address all material vulnerabilities if identified. If a licensee chooses to build its own DC, an assessment of threats and vulnerabilities should be performed at the feasibility stage of the project.

17.6 Appropriate controls deemed acceptable to ensure adequate physical security are as follows:

17.6.1 Access to the DC should be granted on a restricted basis and only to authorized staff. Such access should only be granted on a need to have basis. Physical access of staff to the DC should be revoked immediately when no longer required;

17.6.2 For non-DC personnel such as vendors, system administrators or engineers, who may require temporary access to the DC to perform maintenance or repair work, there should be proper notification of and approval for such personnel during required visits. Licensees should ensure that visitors are accompanied at all times by an authorized employee while in the DC; and

17.6.3 Licensees should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the DC. Physical security measures should be established to prevent unauthorized access to systems, equipment racks and tapes.

18. DATA CENTER RESILIENCY

18.1 To achieve DC resiliency, licensees should assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications. To accomplish this licensees should ensure that:

18.1.1 The DC environment is rigorously controlled and regulated. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical to ensuring uptime and system reliability. Any abnormality detected should be promptly escalated to management and be resolved in a timely manner;

18.1.2 Appropriate fire protection and suppression systems have been implemented in the DC to control a full scale fire if it occurs. Smoke detectors and hand-held fire extinguishers should be installed in the DC and implement passive fire protection elements, such as fire walls around the DC, to restrict the spread of a fire to a portion of the facility; and

18.1.3 To ensure there is sufficient backup power, licensee should install backup power that consists of uninterruptible power supplies, battery arrays, and/or diesel generators.

19. ONLINE FINANCIAL SERVICES[7]

19.1 Core expectations for online financial services are anticipated to include the following:

[7] Supervisory guidance relating to management of online financial services is provided in the Central Bank's ***Guidelines for Electronic Banking***.

19.1.1 Risk and associated controls are expected to be assessed on the type and nature of the online financial services being offered by the licensee. Typically, financial services offered via the internet can be classified into information services, interactive information exchange services and transactional services;

19.1.2 Sensitive or confidential information stored on and accessed by mobile devices should be encrypted to ensure the confidentiality and integrity of this information in storage and transmission;

19.1.3 Processing of sensitive or confidential transaction and customer information should occur in a secure environment; and

19.1.4 Licensees should take steps to educate customers on security measures to protect their own mobile devices from viruses and other errant software which could lead to malicious damage and have harmful consequences.

IT SECURITY

20. TECHNOLOGY HARDWARE AND SOFTWARE

20.1 Steps should be taken by licensees to maintain adequate levels of supported hardware and software to support business functions.

20.2 Effective practices over managing technology hardware and software include the following practices:

20.2.1 To facilitate the tracking of IT resources, licensees should 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;

20.2.2 The licensee should actively manage IT systems and software so that out dated and unsupported systems which significantly increase its exposure to security risks are replaced on a timely basis. Close attention should be paid 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; and

20.2.3 Licensees should establish a technology refresh plan to ensure that systems and software are replaced in a timely manner. Risk assessments should be conducted for systems approaching EOS dates to assess the risks of continued usage and establish effective risk mitigation controls where necessary.

21. NETWORK AND SECURITY CONFIGURATION MANAGEMENT

21.1 Licensees should configure IT systems and devices with security settings that are consistent with the expected level of protection. Licensees 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. These standards include the following measures:

21.1.1 Regular enforcement checks to ensure that 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;

21.1.2 Deployment of anti-virus software to servers, if applicable, and workstations. Anti-virus definition files should be regularly updated and automatic anti-virus scanning on servers and workstations should be performed on a regular basis;

21.1.3 Installation of network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical junctures in its IT infrastructure to protect the network perimeters. Firewalls should be deployed, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or cross-border systems, as well as from the internal trusted network;

21.1.4 Backing up and reviewing rules on network security devices, on a regular basis, to be able to determine that such rules are appropriate and remain relevant; and

21.1.5 Being aware of the risks associated with Wireless Local Area Networks (WLANs) deployed within the organization. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorized access.

22. VULNERABILITY ASSESSMENT AND PENETRATION TESTING

22.1 Vulnerability assessment (VA) is the process of identifying and assessing security vulnerabilities in a system. Licensees should conduct VAs regularly to detect security vulnerabilities in the IT environment. To accomplish this, licensees should:

22.1.1 Deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting;

22.1.2 Establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to confirm that gaps are fully addressed; and

22.1.3 Carry out penetration tests in order to conduct an in-depth evaluation of the security posture of systems through the testing of actual attacks on the system. The licensee should conduct penetration tests on internet-facing systems at least annually.

23. PATCH MANAGEMENT

23.1 Licensees should establish and ensure that the patch management procedures include the identification, categorization and prioritization of security patches. To implement security patches in a timely manner, licensees should establish the implementation timeframe for each category of security patches.

23.2 The application of patches, if not carried out appropriately, could potentially impact other peripheral systems. As such, licensees should perform rigorous testing of security patches before deployment into the production environment.

24. SECURITY MONITORING

24.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorized or malicious activities by internal and external parties, licensees should establish appropriate security monitoring systems and processes by:

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

24.1.2 Implementing security monitoring tools that enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes;

24.1.3 Performing real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications;

24.1.4 Regularly reviewing security logs of systems, applications and network devices for anomalies; and

24.1.5 Adequately protecting and retaining system logs to facilitate any future investigation. When determining the log retention period, licensees should take into account statutory requirements for document retention and protection.

25. ACCESS CONTROLS

25.1 Controlling access is essential to protecting system resources against inappropriate or undesired user access.

25.2 Access controls deemed acceptable are as follows:

25.2.1 Only granting access rights and system privileges based on job responsibility and the necessity to have them to fulfil one's duties;

25.2.2 Verifying that no person by virtue of rank or position have any intrinsic right to access confidential data, applications, system resources or facilities;

25.2.3 Only allowing staff with proper authorization to access confidential information and use system resources solely for legitimate purposes;

25.2.4 Only granting user access to IT systems and networks on a need-to-use basis and within the period when the access is required;

25.2.5 Ensuring that the resource owner duly authorizes and approves all requests to access IT resources;

25.2.6 Subjecting external employees who are given authorized access to critical systems and other computer resources, to close supervision, monitoring and access restrictions similar to those expected of its own staff;

25.2.7 Ensuring that records of user access are uniquely identified and logged for audit and review purposes. This assists with accountability and identification of unauthorized access;

25.2.8 Performing regular reviews of user access privileges to verify that privileges are granted appropriately and according to the ‘least privilege’ principle. This can assist with the identification of wrongly provisioned, redundant, toxic or unnecessary access;

25.2.9 Enforcing strong password controls over users’ access to applications and systems. Password controls should include a change of password upon first logon, minimum password length and history, password complexity as well as maximum validity period. Passwords represent the first line of defence, and if not implemented appropriately, they can be the weakest link in the organization;

25.2.10 Ensuring that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities;

25.2.11 Ensuring that any person who needs to access backup files or system recovery resources is duly authorized for a specific reason and a specified time only. Licensees should only grant access for a specific purpose and for a defined period;

25.2.12 Ensuring that system administrators, IT security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on critical systems they maintain or operate by virtue of their job functions and privileged access. Hence, licensees should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions; and

25.2.13 Closely supervising staff with elevated system access entitlements and having all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. Adoption of the following controls and security practices are recommended:

a) Implement strong authentication mechanisms such as two-factor authentication for privileged users;

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;

i) Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and

j) Protect backup data from unauthorized access.

26. PAYMENT CARD SECURITY

26.1 Payment cards allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase their items over the internet, through mail-order or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines (ATMs) or merchants.

26.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including ATMs, payment kiosks and EFTPOS (electronic funds transfer at point of sale) terminals.

26.3 Types of payment card fraud include counterfeit, lost/stolen, card-not-received (CNR) and card-not-present (CNP) fraud.

26.4 Licensees that provide payment card services should implement adequate safeguards to protect sensitive payment card data. Licensees should ensure that sensitive payment card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission, and the processing of sensitive or confidential information is done in a secure environment.

26.5 Licensees should deploy secure chips to store sensitive payment card data. Licensees should also implement strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (CDA) methods for online and offline card transactions. As magnetic stripe cards are vulnerable to card skimming attacks, licensees should ensure that magnetic stripes are not used as a means to store sensitive or confidential information.

26.6 As it relates to payment cards, licensees should ensure that adequate controls are implemented to manage transactions (for interoperability reasons), where transactions could only be effected by using information from the magnetic stripe on a card.

26.7 For transactions that customers perform with their ATM cards:

26.7.1 Licensees should only allow online transaction authorization;

26.7.2 The licensee card issuer, and not a third party payment processing service provider, should perform the authentication of customers' sensitive static information, such as PINs or passwords; and

26.7.3 The licensee should perform regular security reviews of the infrastructure and processes being used by its service providers.

26.8 Licensees should ensure that security controls are implemented at payment card systems and networks.

26.9 Licensees should only activate new payment cards sent to a customer via post upon obtaining the customer’s instruction.

26.10 Licensees should implement a dynamic one-time-password (OTP) for card not present (CNP) transactions via internet to reduce fraud risk associated with CNP. These transactions present a high risk for fraud and include transactions such as phone, fax, internet and mail order transactions whereby cards are not physically present.

26.11 To enhance card payment security, licensees should promptly notify cardholders via transaction alerts when withdrawals / charges exceeding customer-defined thresholds made on the customers’ payment cards. The licensee should include in the transaction alert, information such as the source and amount of the transaction.

26.12 Licensees should implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities. Licensees 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.

26.13 Licensees should follow up on transactions exhibiting behavior which deviates significantly from a cardholder’s usual card usage patterns. Licensees should investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

TECHNOLOGY RISK MANAGEMENT AND AUDIT

27. IT AUDIT

27.1 As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for licensees to develop effective internal control systems to manage technology risks. It is expected that:

27.1.1 IT audit provides the board of directors and senior management with an independent and objective assessment of the effectiveness of controls that are applied within the IT environment to manage technology risks; and

27.1.1 Licensees should establish an organizational structure and reporting lines for IT audit in a way that preserves the independence and objectivity of the IT audit function.

28. AUDIT PLANNING AND REMEDIATION TRACKING

28.1 The following is expected to support the effective execution and follow up of an IT audit:

28.1.1 Licensees should ensure that the scope of IT audit is comprehensive and includes all critical IT operations;

28.1.2 An IT audit plan, comprising auditable IT areas for the coming year, should be developed. The IT audit plan should be approved by the licensee's Audit Committee;

28.1.3 Licensees should establish an audit cycle that determines the frequency of IT audits. The audit frequency should be commensurate with the criticality and risk of the IT system or process; and

28.1.4 A follow-up process is in place 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, should be established.

*****END*****

APPENDICES

The following appendices provide more specific guidance regarding more technical areas that should be considered to enhance the control environment and contain risk exposures for licensees.

APPENDIX A
KEY MANAGEMENT & CRYPTOGRAPHY

Data confidentiality refers to the protection of sensitive information from unauthorized access and only allowing authorized access.

To prevent compromise of **data confidentiality,** it is expected that:

- An adequate level of encryption that restricts unauthorized access to data is in place. The encryption level should be commensurate with the type and extent of risk present in networks, systems and operations;
- Licensees should only select encryption algorithms which are well established international standards and which have been subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, reputable security vendors or government agencies;
- Protection and secrecy of cryptographic keys used in encryption remain intact;
- No single individual should know entirely what the keys are or have access to all the constituents making up these keys;
- All keys should be created, stored, distributed or changed under the most stringent conditions;
- The sensitivity of data and operational criticality should determine the frequency of key changes;
- Only cryptographic methods that assure sufficient protection of encryption keys and confidential data in an end-to-end authentication operation should be employed; and
- The encryption security pertaining to a customer's PIN and other sensitive data should be maintained end-to-end at the application layer. This means the encryption process is kept intact from the point of data entry to the final system destination where decryption and/or authentication take place.

APPENDIX B
AUTHENTICATION OF CLIENTS AND TRANSACTIONS

System integrity refers to the accuracy, reliability and completeness of information processed, stored or transmitted between the licensees and its customers. A high level of system and data integrity should be achieved consistent with the type and complexity of online services provided.

To prevent compromise of **system integrity,** it is expected that:

- There are monitoring or surveillance systems in place to provide alerts when there are erratic system activities or unusual online transactions;
- There is adequate logical access security that prevents and detects unauthorized access to system data;
- There is adequate physical access security that restricts who can physically access system resources, data assets and storage media. Access to such resources should be selective and on a need-to-access basis;
- There is adequate preventative, detective and corrective controls over the processing and transmission of data within internal and external networks and systems. This would include controls over data input, processing, communication, transmission, output, storage and retrieval of data; and
- Controls established should remain intact when data is at rest, during transmission and in storage.

Customer and Transaction Authenticity

Secure authentication methods should be leveraged to validate the claimed identity of a customer by verifying "what the customer knows" (usually a password or personal identification number) and "what the customer has" (such as a hardware device which generates one-time-passwords at pre-determined time intervals or a USB token which contains a digital certificate and its associated private key).

To ensure customer and **transaction authenticity,** it is expected that:

- Strong customer authentication steps are required before access to customer accounts is granted or transactions are authorized. Protocols and functions such as TripleDES, AES, RC4, IDEA, RSA, ECC, OATH and RFC 2104 HMAC can be employed to help achieve this;
- Customers should provide their User ID and PIN combination and a one-time password (OTP), dynamic access code or digital signature so that their identity and authenticity could be verified before access to their accounts is permitted;
- Two factor authentication (or equivalent) should be required at system login and transaction authorization. Such authentication can be based on any two of the following factors:

  - What you know? (e.g. PIN)
  - What you have? (e.g. OTP token)
  - Who you are? (e.g. Biometrics);

- Two factor authentication protects against phishing, key logging, spyware, malware, middleman attacks and other internet-based scams and malevolent exploits targeted at licensees and their customers;
- Licensees should also require the repeated use of the second authentication factor (e.g. one-time-passwords) by the customer for high value transactions or for changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details) during a login session;
- An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. This assists with protecting communication sessions between the customer and the licensees;
- In the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means;
- New and existing cipher algorithms should be evaluated for sufficiency and enhanced or replaced when deemed required;
- Confirmatory second channel procedures should be applied in respect of transactions above pre-set values, creation of new account linkages, and registration of third party payee details, changing account details or revision to funds transfer limits; and
- Customers could also authenticate the licensee’s web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes or the secure sockets layer (SSL) server certificate verification.

(It should be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.)

APPENDIX C
PERSONNEL MANAGEMENT

Human Resource Management

Internal sabotage, underground espionage or furtive attacks by trusted employees, contractors and vendors are potentially among the most serious risks that a licensees faces. Current and past employees, contractors, vendors and those who have an intimate knowledge of the inner workings of the licensee’s systems, operations and internal controls have a significant advantage over external attackers. A successful attack could potentially jeopardize customer confidence in a licensee’s internal control systems and processes.

Some of the common tactics used by insiders include planting logic bombs; installing stealth scripts; creating system backdoors to gain unauthorized access; as well as sniffing and cracking passwords. System administrators, IT security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the internet banking systems they maintain or operate by virtue of their job functions and privileged access.

Personnel selection and training

Personnel responsible for supporting internet operations and security functions and systems should:

- Have their duties and access to systems resources scrutinized and properly authorized before such access is granted;
- Be hired using stringent selection criteria and thoroughly screened; and
- Be provided adequate training in security principles and practices for personnel involved in developing, maintaining and operating websites and systems.

Execution of duties

- Sensitive and critical system functions and procedures should be jointly carried out by more than one person (dual control) or performed by one person and immediately checked by another (maker/checker).
- Sensitive and critical functions include systems initialization, network security configuration, access control system installation, changing operating system parameters, implementing firewalls and intrusion prevention systems, modifying contingency plans, invoking emergency procedures, obtaining access to backup recovery resources as well as creating master passwords and cryptographic keys.
- Certain functions should be segregated to effectively maintain internal control. Responsibilities and duties that should be separated and performed by different groups of personnel are operating systems function, systems design and development, application maintenance programming, computer operations,

database administration, access control administration, data security, librarian and backup data file custody.

- Where feasible, it is recommended that job rotation and cross training for security administration functions are instituted.
- Transaction processes should be designed so that no single person could initiate, approve, execute and enter transactions into a system in a manner that would enable fraudulent actions to be perpetrated and processing details to be concealed.
- Access rights and system privileges should be based on job responsibility and the necessity to have the privileges in order to fulfil duties.
- It is recommended that no person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization should be allowed to access confidential information and use system resources solely for legitimate purposes.
- No one should have concurrent access to both production systems and backup systems, particularly data files and computer facilities. Any person who needs to access backup files or system recovery resources should be duly authorized for a specific reason and a specified time only. Access which is not for a specific purpose and for a defined period should not be granted. This is also applicable to vendors, service providers and consultants and such external personnel should also be subjected to close supervision, monitoring and access restrictions similar to those applying to internal personnel.
- Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged as they have the inside knowledge and the resources to circumvent systems controls and security procedures.

APPENDIX D
BEST PRACTICES FOR SECURITY

Licensees may leverage the following security best practices to reduce exposure to technology risks. Adoption of the control and security practices listed below is recommended:

- Implement two-factor authentication for privileged users;
- Institute strong controls over remote access by privileged users;
- Restrict the number of privileged users;
- Grant privileged access on a “need-to-have” basis;
- Maintain audit logging of system activities performed by privileged users;
- Ensure that privileged users do not have access to systems logs in which their activities are being captured;
- Conduct regular audit or management review of the logs;
- Prohibit sharing of privileged IDs and their access codes;
- Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
- Protect backup data from unauthorized access.
- Deploy hardened operating systems – systems software and firewalls should be configured to the highest security settings consistent with the level of protection required, keeping abreast of updates, patches and enhancements recommended by system vendors; change all default passwords for new systems immediately upon installation.
- Install firewalls between internal and external networks as well as between geographically separate sites.
- Install intrusion detection-prevention devices (including denial-of-service security appliances where appropriate).
- Develop built-in redundancies for single points of failure which can bring down the entire network.
- Perform application security review using a combination of source code review, stress loading and exception testing to identify insecure coding techniques and systems vulnerabilities.
- Engage independent security specialists to assess the strengths and weaknesses of internet-based applications, systems and networks before each initial implementation, and at least annually thereafter, preferably without forewarning to internal staff who are operationally or functionally responsible for the system or activity.
- Conduct penetration testing at least annually.

- Establish network surveillance and security monitoring procedures with the use of network scanners, intrusion detectors and security alerts.
- Implement anti-virus software.
- Conduct regular system and network configurations review and data integrity checks.
- Maintain access security logs and audit trails.
- Analyse security logs for suspicious traffic and intrusion attempts.
- Establish an incident management and response plan.
- Test the predetermined response plan relating to security incidents.
- Install network analysers which can assist in determining the nature of an attack and help in containing such an attack.
- Develop and maintain a recovery strategy and business continuity plan based on total information technology, operational and business needs.
- Maintain a rapid recovery capability.
- Conduct security awareness education and programs.
- Require frequent ICT (information and communication technology) audits to be conducted by security professionals or internal auditors who have the requisite skills.
- Consider taking insurance cover for various insurable risks, including recovery and restitution costs.
- Provide separate physical/logical environments for systems development, testing, staging and production; connect only the production environment to the internet.
- Implement a multi-tier application architecture which differentiates session control, presentation logic, server side input validation, business logic and database access.
- Implement two-factor authentication at login for all types of internet banking systems and a specific OTP (one-time password) or digital signature for each value transaction above a specified amount selectable by the customer or predetermined by the licensees.
- Deploy strong cryptography and end-to-end application layer encryption to protect customer PINs, user passwords and other sensitive data in networks and in storage.
- Encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

  a) Deploy strong user authentication in wireless local area networks and protect sensitive data with strong encryption and integrity controls.