BANK OF GUYANA

SUPERVISION GUIDELINE NO. 15

ISSUED UNDER THE AUTHORITY OF THE FINANCIAL INSTITUTIONS ACT 1995

(NO. 1 OF 1995)

TECHNOLOGY RISK MANAGEMENT

January 2024

Contents

ACRONYMS

ATMs	Automatic Teller Machines
CISO	Chief Information Security Officer
CNP	Card-Not-Present
CNR	Card-Not-Received
DCs	Data Centres
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSS	Data Security Standard
EOS	End-Of-Support
FIA	Financial Institutions Act
ICT	Information and Communications Technology
IP	Internal Protocol
ISO	International Organization for Standardization
IT	Information Technology
LFIs	Licensed Financial Institutions
NIST	National Institute of Standards and Technology
OTP	One-Time-Password
PINs	Personal Identification Numbers
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	System Development Life Cycle
SQL	Structured Query Language
TCP	Transmission Control Protocol
TRM	Technology Risk Management
UAT	User Acceptance Testing
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

GLOSSARY

Terms	Definition
Abnormal system activities	An example of abnormal system activities includes multiple sessions using an identical customer account originating from different geographical locations within a short time span.
Built-in redundancies	the duplication of critical components of the system, to reduce single points of failures.
CNP fraud	is a fraudulent transaction where neither the card nor the cardholder is present whilst conducting the transactions.
CNR fraud	relates to the interception of genuinely issued cards before they reach the authentic customers. Impostors then use intercepted cards fraudulently.
Counterfeit card fraud	is perpetrated with a card that has been illegally manufactured using information stolen from the magnetic strip of a genuinely issued card.
Cross-site scripting	a type of injection security attack in which an attacker injects data, such as a malicious script, into content from otherwise trusted websites.
Data at endpoint	data which resides in notebooks, personal computers, portable storage devices and mobile devices.
Data at rest	data in computer storage which includes files stored on servers, databases, back-up media and storage platforms.
Data commingling	occurs when different items or kinds of data are stored in such a way that they become commonly accessible when they should remain separated.
Data in motion	data that traverses a network or that is transported between sites.
DoS and DDoS attack	A DoS attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. Whereas, a DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once.
E-banking	is the provision of banking products and services through electronic channels. E-banking includes banking via the internet, phone, automated teller machines (ATMs), and any other electronic channel.
Escalation and response plan	a set of instructions to help IT detect, respond to, and recover from computer network security incidents such as data loss or cybersecurity breaches.
Escrow agreement	a contract that outlines the terms and conditions between parties involved, and the responsibilities of each. Escrow agreements generally involve an independent third party, referred to as an escrow agent, who holds an asset of value until the specified conditions of the contract are met.

Terms	Definition
ICT	is the convergence of computing, telecommunication and governance policies for how information should be accessed, secured, processed, transmitted and stored.
Information service	is the most basic form of online internet service. It is a one-way communication whereby information, advertisements or promotional material are provided to the customers.
Information system assets	are information-system components, or a part of the information system that support the business assets. They also act as indicators of the significance of the security risk.
Interactive information exchange service	allows customers to communicate with the FI, make account enquiries and fill in application forms to take up additional services or purchase new products offered.
IT assets	assets that are managed, developed or supported by a technology function, service providers or teams/individuals located within business units are components of IT assets.
IT incident	occurs when there is an unexpected disruption to the standard delivery of IT services.
IT steering committee	generally consists of business owners, the development team and other stakeholders.
Internet insurance	is the use of the internet as a channel to transact insurance business with customers or as a platform for transmission of customers' information.
Lost/stolen card fraud	is a fraudulent transaction that occurred on a valid issued card after a cardholder lost his/her card or was stolen from the legitimate owner.
Man-in-the-middle attack (MITMA)	an interloper is able to read, insert and modify messages between two communicating parties without either one knowing that the link between them has been compromised. Possible attack points for MITMA could be customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the customer and the FI's server.
Multi-tenancy	allows for customers to share the same hardware resources, by offering them one shared application and database instance, while allowing them to configure the application to fit their needs as if it runs on a dedicated environment. It allows customers to enjoy economies of scale as a result of multiple customers - "tenants" - sharing the same application and database instance.
Non-production environment	refers to information processing systems used for any purpose other than live use such as performance and systems testing.
OTP	is a password that is valid for only one login session or transaction, on a computer system or other digital device.

Terms	Definition
Payment cards	refer to ATM, credit, charge and debit cards.
Physical/logical environment	refer to the tangible aspects of information resources such as computer hardware while a logical environment includes the data and processing aspects of the IT Department.
Physical or logical intrusion	involves the physical access of an intruder into an organization to steal information assets or carry out sabotage, for example, the intruder might try to remove hard disks whereas logical Intrusion refers to unauthorized access to software or data without physical damage to an information system, for example, damaging or stealing data and installation of bug or wiretapping.
Production IT environment	the infrastructure, hardware, software, and systems that a business relies on every day in the course of using IT. Some of the commonly used resources in an IT environment include computers, internet access, peripheral devices, etc.
Program migration	involves the movement of software codes and scripts from the development environment to the test and production environment.
Risk appetite	is the amount and type of risk that an institution is willing to pursue or retain[1].
Risk tolerance	defines the level and nature of risks to which the BOD of the LFI considers acceptable to expose the institution.
RPO	the acceptable amount of data loss, for IT systems and applications.
RTO	the duration of time from the point of disruption to system restoration.
Source code reviews	are designed to identify security vulnerabilities and deficiencies, and mistakes in system design or functionality.
SQL injection	a computer attack in which malicious code is embedded in a poorly-designed application and then passed to the backend database. The malicious data then produces database query results or actions that should never have been executed.
Technology management best practices	this includes: (a) clear definition of the roles and responsibilities of staff involved in the project; (b) ensuring processes for developing or acquiring new systems are present; (c) utilizing project plans for all IT projects; (d) ensuring 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) ensuring there is project management oversight monitoring so that milestones are reached and deliverables are realized on a timely basis.

[1] ISO Guide 73:2009 Risk Management – Vocabulary

Terms	Definition
Transactional service	allows customers to execute online transactions such as the transfer of funds, payment of bills and other financial transactions.
Two-factor authentication	for system login can be based on any two of the factors, i.e., what you know (e.g. PIN), what you have (e.g. OTP token) and who you are (e.g. Biometrics.

PART I - INTRODUCTION

1. The Bank of Guyana (hereinafter referred to as the Bank) in furtherance of its responsibility for the regulation and supervision of licensees under the FIA 1995, has developed this Guideline to provide direction to LFIs on what is required to implement an adequate Technology Risk Management (TRM) Framework and to guide the conduct of IT reviews/examinations.

2. The advancement of information technology has brought about rapid changes to the way businesses and operations are being conducted in the financial industry. It has also allowed great opportunities for LFIs to provide new services and products. IT has moved from the traditional support function to a pivotal component in businesses' interaction with their customers.

3. LFIs are expanding their use of online systems, such as internet banking systems, mobile banking and payment systems. Consequently, LFIs should completely understand the magnitude and intensification of technology risks from these systems and put measures in place for an adequate and robust risk management system as well as operating processes to manage these risks. The measures suggested for implementation cannot be static. LFIs need to proactively create/modify their policies, procedures and technologies based on new developments and emerging concerns.

4. The risk management principles and best practice standards are as follows:
   a) Establishing a sound and robust technology risk management framework;
   b) Strengthening system security, reliability, resiliency, and recoverability; and
   c) Deploying strong authentication to protect customer data, transactions and systems.

5. Effective enforcement of this guideline will minimize the risks associated with technology, thereby enhancing the integrity of the financial system.

Applicability

6. This Guideline applies, as appropriate, to all LFIs.

7. The extent to which a LFI implements the Guideline should be commensurate with its size, risk profile and business model.

8. Any deviation from this Guideline must be explained in a separate document, to be made promptly available to the Bank. In addition, LFIs are required to ensure the security of all the LFI's and customer's assets by an acceptable proven alternative, relative to an agreed and established maturity level between the Bank and the LFI.

Supervisory Approach

9. The Bank's supervisory approach is not a prescriptive and comprehensive approach for all technology risks. However, it aims to provide LFIs with general guidance to address the risks involved with technology usage for their business operations. A keenness for sound practices and processes for managing all the technology risks is the objective of this guideline.

Risks Categories

10. Technology risks can be identified in the five following categories:

    a) *Availability and continuity risk*: the risk that the performance and availability of systems and data are adversely impacted, including the inability to timely recover due to a failure of hardware or software, management weaknesses, or any other event.

    b) *Data integrity risk*: the risk that data stored and processed are incomplete, inaccurate or inconsistent across different systems.

    c) *Change risk*: the risk arising from the inability of the institution to manage system changes in a timely and controlled manner.

    d) *Outsourcing risk*: the risk that engaging a third party, or another group entity (intra-group outsourcing), to provide systems or related services, adversely impacts the institution's performance and risk management

e) *Security risk*: the risk of unauthorized access to systems from within or outside the institution[2].

IT Risks

11. To aid the risk profile process, an insight in IT risks may be useful. 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 telecommunications systems are technology risks.

12. 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 can also be associated with these risks.

13. Given the increased usage and wide reaching nature of technology, it also includes the risk of loss from inadequate or failed internal processes, people, systems, or external events impacting IT assets.

14. Further, IT's extensive reach, if significantly compromised could cause operational harm such as an organization's ability to meet overall business objectives. In addition, IT risks from a security standpoint is compromised when there is a breach of the following:

a) *Confidentiality* – where there is unauthorized access to data and systems;

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

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

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

[2] Toronto Centre. Supervision of Cyber Risk. December 2018. https://res.torontocentre.org/guidedocs/Supervision%20of%20Cyber%20Risk%20FINAL.pdf

PART II - GOVERNANCE FRAMEWORK

Oversight of Technology Risks by Board of Directors and Senior Management

16. The importance of technology to the functioning of a LFI cannot be stressed enough, as such the Board and Senior Management[3] should have oversight of technology risks to ensure that the organization's IT functions are aligned with and capable of supporting the LFI's business strategies and objectives.

17. For effective oversight of the IT risks, the Board must have a comprehensive understanding of the potential risks[4] technology presents to the institution, seek further clarification from management so that there is an almost precise picture of the risk profile and ensure that there are clearly defined mandates to guide operations.

Roles and Responsibilities

18. The Board of Directors and Senior Management need not be IT experts but should have sufficient knowledge to oversee and challenge management and to execute their roles and responsibilities.

19. **The Board is responsible for ensuring:**

a) that the IT strategy is aligned with the overall business strategy;

b) the establishment and ongoing maintenance of a robust technology risk management framework;

c) that they are involved in key IT decisions;

d) that there are effective internal controls and risk management practices in place to achieve ongoing security, reliability, resiliency and recoverability;

e) the instillation of organizational committees or similar frameworks[5].

f) that the following roles and responsibilities of senior management are complied with, and that the corresponding risk tolerance is understood.

[3] See Appendix 1 for a proposed IT Governance Structure.
[4] See Appendix 2 for some significant risks.
[5] Appendix 1 also gives examples of these committees.

20. **Senior Management should in relation to:**

a. IT Policies, Standards and Procedures

i. Establish technology policies, standards and procedures that govern the management of technology risks and safeguard the licensee's information system assets;

ii. Ensure that the LFI has a cyber-security policy based on its risk profile and address cyber risk threats to the extent applicable to its operations;

iii. Regularly review and update policies, standards and procedures or at least annually to ensure that documents remain relevant to current threats and technologies;

iv. Implement and execute 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;

v. Ensure that there is adequate assessment of the cost-benefit analysis of the technology investment such as the investment in IT controls and security systems, networks, and DCs, operations and backup facilities, taking into account reputational risk, customer confidence, consequential impact and legal implications; and

vi. Monitoring and evaluating existing and future trends in technology that may impact the business strategy, including monitoring of overall industry trends.

21 ***b. Human Resource Criteria***

i. Implement 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. The screening for vendors and contractors may include but not be limited to the following:

- Professional reference(s); and
- Technical track record.

ii. Ensure that staff, vendors and contractors, who are authorized to access licensee systems, are formally required to protect sensitive or confidential information.

22 ***c*. *IT Security Awareness***

i. Implement a comprehensive IT security awareness training program that is endorsed by senior management which should include information on IT security policies and standards as well as individual responsibility with respect to IT security measures that should be taken to safeguard information system assets. The board, management and relevant staff should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources; and

ii. Review and update the training program at least annually to ensure that the contents remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks. Training should be extended to all new and existing staff.

23 ***d. Reporting of Security Incidents***

Inform the Board of technology risk developments and incidents that may have a significant impact on the LFI in a timely manner.

Technology Risk Management Framework

24 The LFI's TRM framework should be established to manage technology risks in an efficient, effective and consistent manner. The framework may include, but should not be limited to the following:

a) Clear roles and responsibilities in managing technology risks;

b) Identification and prioritization of information system assets;

c) Identification and assessment of the impact and likelihood of current and emerging threats, risks and vulnerabilities;

d) Implementation and monitoring of appropriate practices and controls to mitigate risks; and

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

25 To ensure the risk management framework is effective, it must be able to identify the information system assets that need protection; identify both direct and indirect IT threats; calculate the probability and potential impact of identified risks; for each identified risk evaluate, prioritize and implement appropriate risk reduction controls; and facilitate the maintenance and reporting of valuable risk metrics that are periodically provided to the appropriate levels of management.

26 The following are key components of effective risk management:

a) Risk Identification

This involves:

i. Identification and critical 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;

ii. 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, system interfaces, operations and human elements;

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

iv. Vigilant monitoring of emerging security risks such as DoS attacks, internal sabotage and malware infestation, or other forms of cyber threat.

27 b) Risk Assessment

This involves:

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

ii. 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;

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

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

28 Risk Mitigation and Control

This involves:

i. The development and implementation of risk mitigation and control strategies that are consistent with the value of the information system assets and risk tolerance limits.

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

iii. A methodical approach for evaluating, prioritizing and implementing appropriate risk-reduction controls. It is a combination of technical, procedural, operational and functional controls that would provide a rigorous mode of reducing risks;

iv. Prioritizing threat and vulnerability pairings with high-risk ranking. Parings with high-risks could cause significant harm or impact to the LFI's operations, as it may not be practical to address all known risks simultaneously or in the same timeframe. The LFIs should assess its risk tolerance for damages and losses in the event that a given risk-related event materializes. When deciding on the adoption of alternative controls and security measures, the LFI should also be conscious of costs and effectiveness of the controls with regard to the risks being mitigated;

v. Managing and controlling risks in a manner that will maintain its financial and operational viability and stability; and

vi. Refraining from implementing and running a system where the threats to the safety and soundness of the IT system are insurmountable and the risks cannot be adequately controlled.

29 Risk Monitoring and Reporting

This involves:

i. Maintenance of an inventory of risks and controls applicable to the licensee, which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. LFIs should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks;

ii. 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;

iii. Implementing IT risk 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; and

iv. Periodically reviewing and updating risk management processes, re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes.

PART III - IT OPERATIONS AND CONTROLS

Management of IT Outsourcing Risks

30 IT outsourcing is the use of external service providers to effectively deliver IT-enabled business process, application service and infrastructure solutions for business outcomes. Some of the most common types of IT outsourcing are in systems development and maintenance, support to DC, network administration, disaster recovery services, application hosting, and cloud computing.

31 As LFIs pursue outsourcing, the following factors should be taken into consideration:

a) An appropriate service provider should be thoroughly scrutinized before acquiring the outsourced service. Management should perform relevant due diligence, evaluate the service provider's proposal in light of the institution's needs, and ensure that selection is done in accordance with the institution's rules/procedures[6];

b) The contractual terms and conditions governing the obligations of the LFI and service provider must be established fully in writing where all requirements are captured. The requirements and conditions covered in the agreements should include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility;

c) 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.

d) Requirement for the service provider to implement security policies, procedures, and controls which should be as stringent as the service provider would expect for their own operations;

e) LFIs should monitor and review the security policies, procedures and controls of the service provider on a regular basis, including commissioning or obtaining

[6] Federal Financial Institutions Examination Council Outsourcing Technology Services Booklet: Service Provider Selection https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/service-provider-selection.aspx

periodic expert reports on security adequacy and compliance in respect of the operations and services provided

f) The financial viability of the LFI's service provider(s) should be determined on an annual basis and reports should be presented to management. Should the institution become aware that the provider's financial condition is becoming unstable, a disaster recovery contingency framework must be implemented. This framework plays a vital role in ensuring that all IT functions of the LFIs continue operating regardless of any negative internal or external shocks to the banking environment. The plan should take into account worse case disruption scenarios and the unavailability of the existing service provider, after which viable alternatives for resuming IT services should be identified. One way to minimize the impact of negative shocks is through the implementation of an escrow agreement between the LFI, the service provider and all other parties involved. This agreement must include detailed procedures to be followed by each party involved should internal or external shocks occur along with the possibility of the service provider completely defaulting on any contractual obligation.

g) Licensees should ensure that the contingency plan is shared with the relevant stakeholders who are sufficiently trained on the recovery plan and execution steps; and

h) The licensee should ensure that there is an exit strategy in place in the event of a termination of the relationship. If the provider remains in operation, its financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. An LFI has several alternatives including obtaining required equipment and software for in-house processing and transferring data files to another provider[7].

[7] Federal Financial Institutions Examination Council Outsourcing Technology Services Booklet: Financial Condition of service Provider https://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services/risk-management/ongoing-monitoring/financial-condition-of-service-providers.aspx?prev=1

System Development Life Cycle (SDLC)

32 SDLC is a project management technique that divides complex projects into smaller, more easily managed segments or phases. Segmenting projects allows managers to verify the successful completion of project phases before allocating resources to subsequent phases[8]. Diagram 1 shows the approach used by the SDLC for an application system or a major modification to that system.

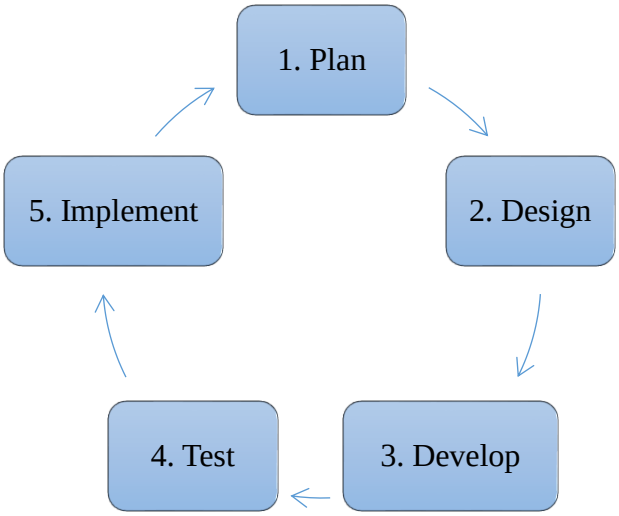


Diagram 1: Uses of SDLC for an Application System

33 The SDLC would then be implemented in various phases which will be thoroughly perused by the licensee. These phases vary from the feasibility study to the post implementation review, however it does not include the service delivery or benefits realization activities as shown in Diagram 2.

[8] Federal Financial Institutions Examination Council Outsourcing Technology Services Booklet: Systems Development Life Cycle

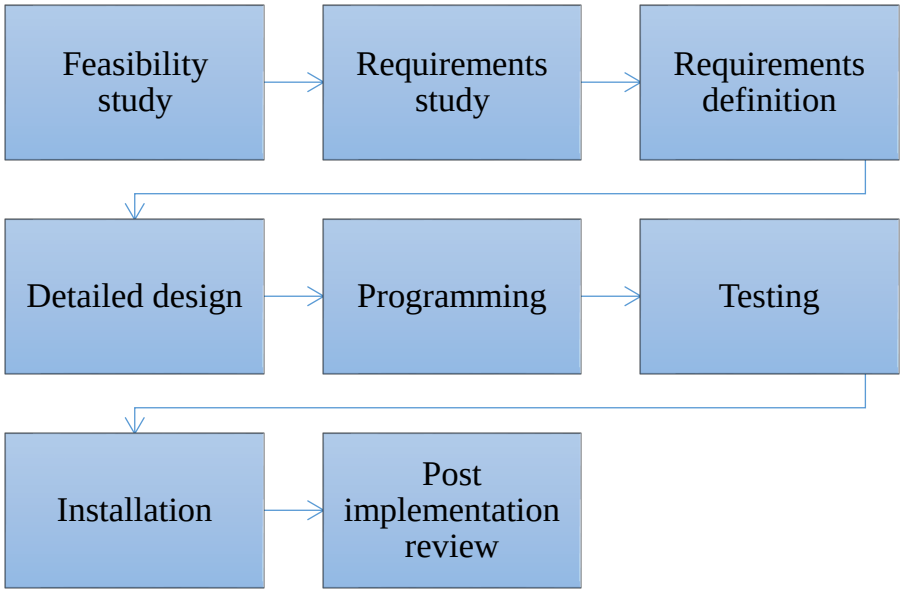


Diagram 2: The Phases of the SDLC

34 There are inherent risks when developing and deploying technology ranging from cost to involvement of business users for proper acceptance of the system. The licensee should therefore evaluate whether there are any deficiencies or defects in the system design, development and testing phases. Effective oversight should occur over the entire SDLC process.

Effective Oversight of the SDLC Process

35 The following should be considered by the licensee:

a) Establishment of an IT Steering Committee;

b) Employing technology management best practices such as:

i. clearly defining the roles and responsibilities of staff involved in the project;

ii. ensuring that all 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;

iii. utilizing project plans for all IT projects, where such plans should identify what deliverable is expected and what milestones are to be accomplished at each phase of the project;

iv. ensuring 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

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

c) Integration and management of security requirements throughout the project lifecycle, which include the following security best practices:

i. Clear specification of security requirements for all aspects of the IT department;

ii. Implementing a system testing methodology where the scope of the tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions;

iii. Ensuring full regression testing is performed before system changes or enhancements are implemented;

iv. Reviewing and signing off on the outcome of the changes by users whose systems and operations are affected by the change being implemented;

v. Conducting penetration testing, which involves testing a computer system to find security vulnerabilities that an attacker can exploit, prior to the commissioning of a new system;

vi. Performing vulnerability scanning of external and internal network components that support new systems; and

vii. Maintaining separate physical or logical environments for unit, integration, system and user-acceptance tests. Additionally, vendor and developers' access to UAT environments should be closely monitored.

d) Customizations of the system may be required for introduction of new functionality and modules to the existing technology environment;

e) Deployment of a source code to support associated technology should be reviewed as source code weaknesses may lead to intentional or unintentional manipulation of a vulnerability by an attacker;

f) Reviewing the source code is recommended to address such concerns. The review should involve a methodical examination of the source code of an application with the objective of identifying defects arising due to coding errors, poor coding practices or malicious attempts. The 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, etc. before the system is implemented. The following are considerations when evaluating the sufficiency of source code deployed:

   i. Confirm that systems have appropriate security controls;

   ii. Conduct a risk analysis of the system and based on the results, customize examinations that rigorously test specific application modules and security safeguards; and

   iii. 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.

g) Developing and implementing adequate business recovery and back-out plans in case of an unsuccessful deployment or significant issue that requires a roll back of the deployment;

h) 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. The following is recommended commensurate with the risk of applicable end-user tools:

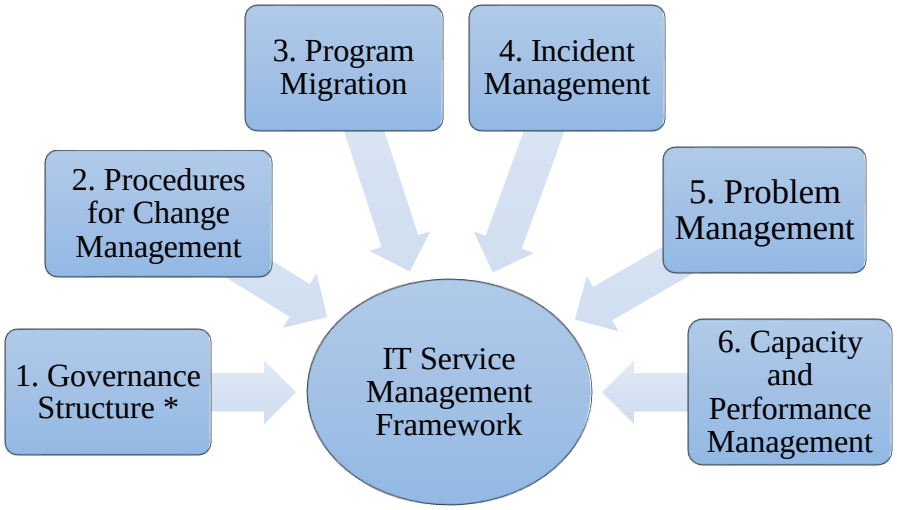
   i. Perform an assessment to ascertain the importance of these applications to the business;

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

iii. Review and test end-user developed program codes and scripts before they are used so as to ensure the integrity and reliability of the applications. This includes change and version management controls.

IT Service Management

36 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.



** Adequately covered in paragraphs 16-23*

Diagram 3: Components of a control framework around IT Service Management

Change Management

37 Taking into consideration the components depicted in Diagram 3 above, it is expected that:

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

b) Such changes should be applied to system and security configurations, hardware devices and software updates;

c) Prior to these changes, risk and impact analysis are performed to the requested changes where assessments can be made to determine how the systems or applications are impacted;

d) Appropriate test plans are developed and implemented to vet the impending changes. 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;

e) All changes to the production environment should be approved by authorized personnel;

f) Back-ups should be performed for affected systems or applications prior to the change in order to minimize risks associated with the changes; and

g) Audit and security logs are enabled to record activities that are performed during the migration process.

Program Migration

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

39 Therefore, to prevent negative outcomes during the migration process, the following best practices are recommended:

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

b) The licensee should perform a risk assessment to ensure that sufficient preventative and detective controls have been implemented before connecting a non-production environment to the internet;

c) Ensure proper segregation of duties is enforced so that no single individual has the ability to make unauthorized decisions such as developing, compiling and moving object codes from one environment to another; and

d) Changes implemented should be migrated to disaster recovery systems or applications for consistency.

Incident Management

40 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 prolonged disruption of IT services. In an attempt to limit or completely prevent any negative IT incidents, the following sound incident management practices should be followed:

a) An incident management framework should be developed aimed at restoring normal IT service promptly following an incident, with minimal impact on the business;

b) Establishing clear roles and responsibilities of staff involved in the incident management process;

c) Assignment of incidents and management based on 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;

d) Establishment and documentation of criteria used for assessing levels of incidents[9];

e) Establishment of escalation and resolution procedures which should be commensurate with the assigned severity level of the incident;

f) The escalation and response plan for security should be tested on a regular basis;

g) Existence of a computer emergency response team, with necessary resources and skills to handle major events;

h) In the event that an incident becomes a crisis, sufficient and timely communication to Senior Management should be made to activate a timely disaster and recovery plan. There should also be immediate communication to the Bank highlighting this incident and the actions taken[10];

i) Incident response procedures should include a predetermined action plan to address public relations issues in order to maintain customer confidence throughout the crisis;

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

---

[9] See Appendix 3 for an Incident Management Reporting template which highlights the criteria used for assessing the incident type and its level of severity.

[10] Appendix 3 can also be used to report incidents to the Bank.

k) Remediation actions are taken as necessary and reported to management and the issue is monitored to closure to prevent the recurrence of similar incidents;

l) Preparation of incident reports which should include an executive summary, analysis of root cause, its impact as well as measures taken/to be taken when addressing the cause and consequences of the incident;

41 The root-cause analysis should cover the following areas:

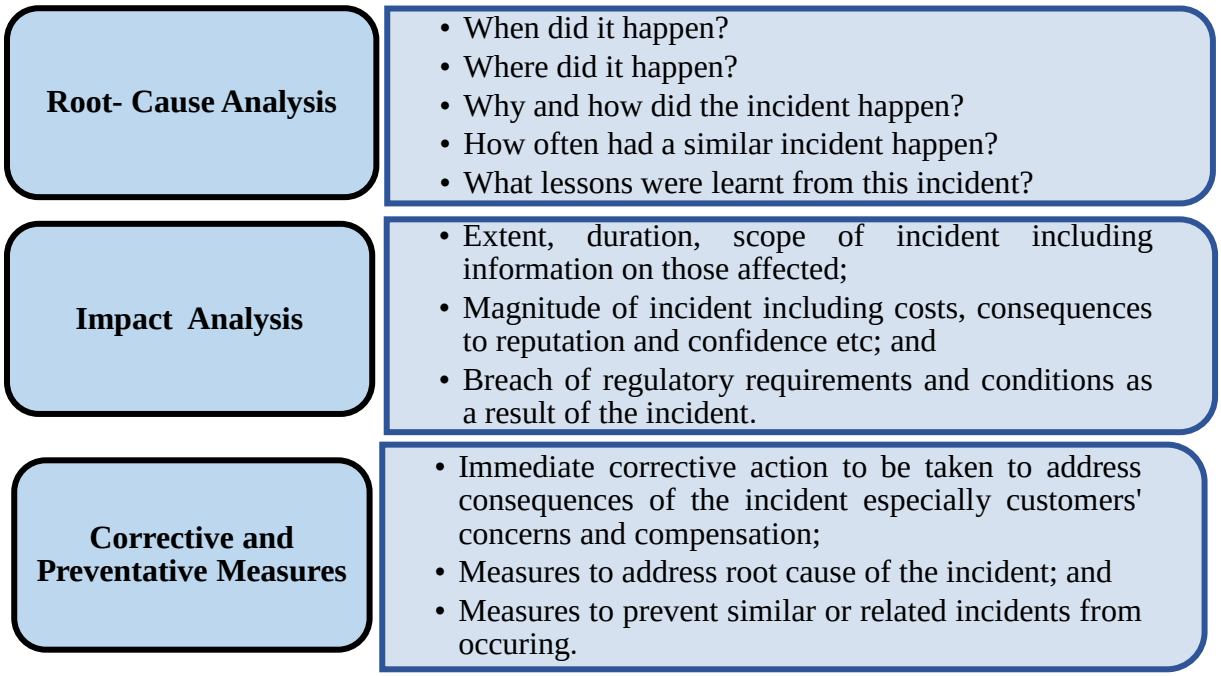


Diagram 4: Components of Root-Cause Analysis

Problem Management

42 The aim of problem management is to determine and eliminate an incident's root cause so as to prevent the occurrence of repeated problems. The diagram below highlights the procedures to be followed in carrying out sound problem management practices.

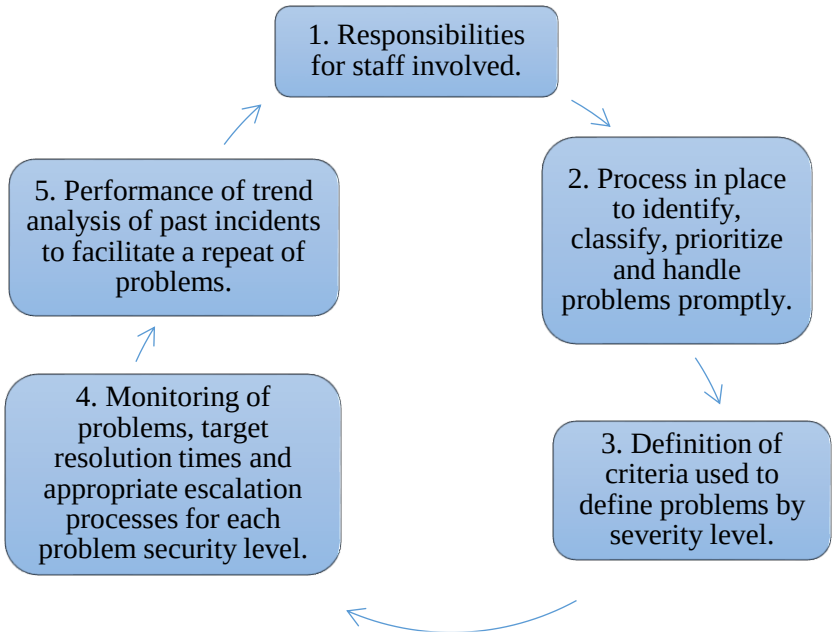


Diagram 5: Sound practices of problem management

Capacity and Performance Management

43 To ensure that IT systems and infrastructure are able to support business functions, licensees should ensure that indicators such as performance, capacity and utilization of the systems are monitored and reviewed. The following diagram depicts sound capacity and performance management practices:

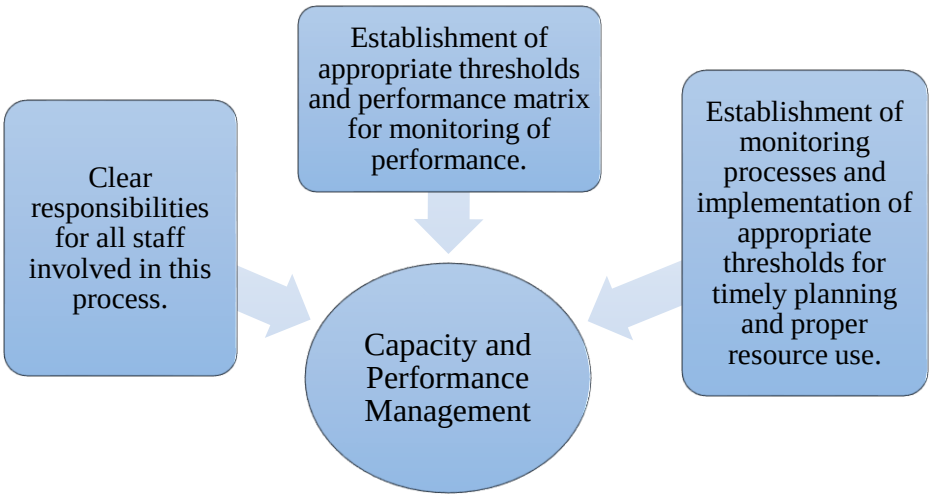


Diagram 6: Best Practices for Capacity Performance Framework

System Reliability, Availability and Recoverability

44 This process entails IT systems, networks and infrastructures that are crucial in maintaining confidence and trust in a licensee's operational and functional capabilities. When critical systems fail, for instance, hardware malfunction, operating errors or security breaches, the disruptive impact on a licensee's operations or their customers will usually be severe and widespread and could lead to serious consequences to the licensee's reputation.

Systems Availability and Disaster Recovery Plan

45 To prevent system failures, the following key points, specific to proper management of IT should be followed:

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

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

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

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

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

f) Licensees should define system recovery and business resumption priorities and establish specific recovery objectives. These include RTO and RPO;

g) 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[11];

h) There are various considerations that determine the speed at which recovery is achieved which includes the importance of 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; and

i) 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.

Disaster Recovery Testing

46 During a system outage, the LFI should refrain from adopting impromptu and untested recovery measures over pre-determined recovery actions that have been rehearsed and approved by management. Ad hoc recovery measures carry high operational risks as their effectiveness has not been verified through rigorous testing and validation. To ensure readiness during outages, licensees should take steps to validate the completeness and adequacy of recovery plans.

[11] Geographically separate refers to the next most appropriate location that is suitable for the location of the recovery site which will allow for immediate and effective resumption of all its operations should any form of disruption occur. There should be adequate distance between the primary and recovery sites in order to minimize the impact of a disaster on the recovery site.

47 The following diagram shows how licensees can achieve this:

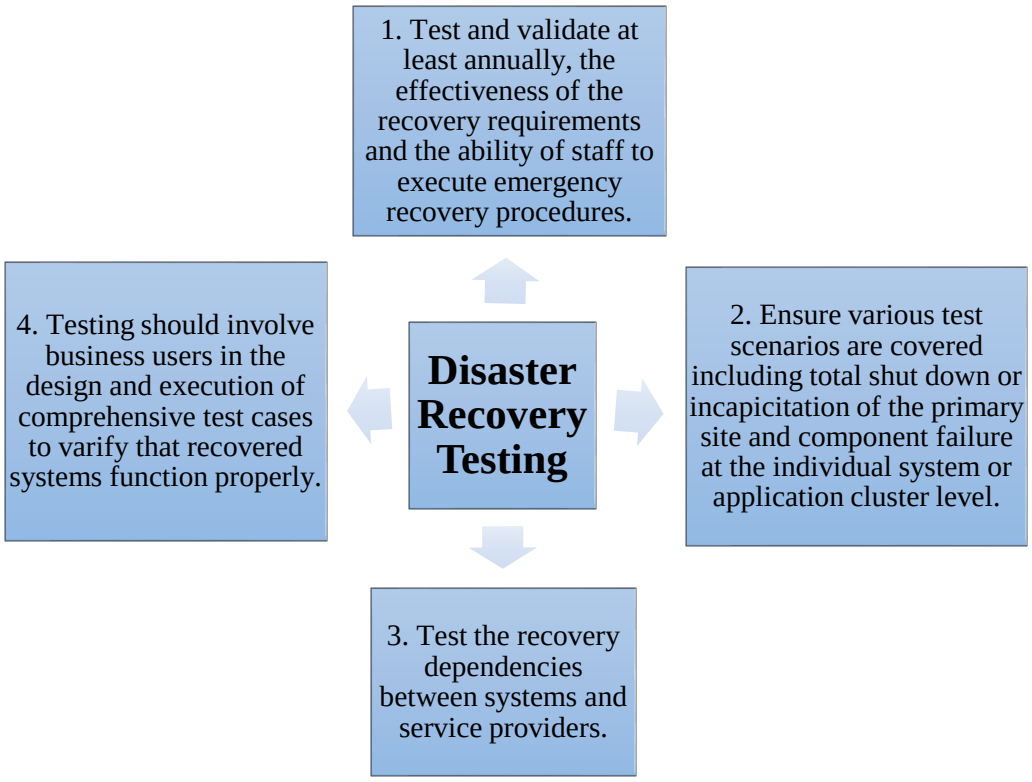


Diagram 7: Steps to validate completeness and adequacy of recovery plans

Data Loss Prevention

48 Appropriate technological measures should be taken to protect sensitive or confidential information such as personal customer information and account and transaction data which are stored and processed in licensees' systems.

49 The following measures may be employed by the licensee in preventing data loss:

a) Identify important data and adopt adequate measures to detect and prevent unauthorized access, copying or transmission of confidential information;

b) The LFI should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information, taking into consideration the following:

i. Data at endpoint;

ii. Data in motion; and

iii. Data at rest.

50 To achieve security of data at endpoints, the LFI should implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres. The LFI should protect confidential information stored in all types of endpoint devices with strong encryption;

51 LFIs should not use unsafe internet services such as social media sites, internet storage sites, and web-based emails to communicate or store confidential information. Appropriate control measures should be in place to detect, prevent and manage the use of such services within the organization;

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

53 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

54 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 sanitation method, LFIs should consider the security requirements of the data residing on the media.

Data Backup Management

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

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

b) Consider the implementation of specific data storage architectures. In this regard, processes should be in place to review the structure and connectivity of information

storage systems to detect any potential points of failure or fragility in its design, as well as ensuring that the technical support by service providers are present;

c) 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

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

Data Centre Protection and Controls

56 Typically, a licensee's critical systems and data are concentrated and maintained in a DC. It is therefore important that the DC is resilient and physically secured from internal and external threats.

Threat and Vulnerability Risk Assessment (TVRA)

57 Appropriate controls expected for data centre protection include performance of a TVRA to identify security threats and operational weaknesses in a DC. This will determine the level and type of protection that should be established to safeguard the data. 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 addressing 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.

Physical Security

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

a) Access to the DC should be granted on a restricted basis and only to authorized staff;

b) 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; and

c) 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.

Data Centre Resiliency

59 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:

a) The DC environment is rigorously controlled and regulated. Any abnormality detected should be promptly taken to management and be resolved in a timely manner;

b) Appropriate fire protection and suppression systems have been implemented in the DC to control a full scale fire if it occurs; and

c) There is sufficient backup power that includes uninterruptible power supply.

Quality Management

60 During project planning, the LFIs should define the expected quality attributes and the assessment metrics for the project deliverables based on its quality control standards.

61 Quality assurance must be performed by an independent quality assurance function to ensure that project activities and deliverables comply with the LFI's policies, procedures and standards.

PART IV - IT SECURITY AND AUDIT

IT Security

Technology Hardware and Software

62 LFIs should maintain adequate levels of supported hardware and software to aid its business functions. Practices surrounding the management of hardware and software should include the following:

a) Facilitating the tracking of IT resources, LFIs 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;

b) Active management of 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. Also, close attention should be paid to the product's 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;

c) Establishment of 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;

d) Monitoring processes should be established and appropriate thresholds implemented to provide sufficient time for the LFI to plan and determine additional resources to meet operational and business requirements effectively;

e) Ensuring that IT systems and infrastructure are able to support business functions, LFIs should ensure that indicators such as performance, capacity and utilization are monitored and reviewed; and

f) Actively monitor technological developments to ensure that the LFI is aware of security risks. LFIs should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.

63 Any significant delays in finding or fixing software with critical vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain.

Network and Security Configuration Management

64 To ensure the security of the information assets, strong network security controls are important. This needs to be enabled by providing authorized access to the internal network using a combination of technology and process controls. Network access controls should be implemented to restrict network traffic to and from systems and devices to prevent a cyber-threat actor from accessing the LFI's network and launching malware or DDoS attacks.

65 IT systems and devices should be configured with security settings that are consistent with the expected level of protection. LFIs 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.

66 In ensuring strong network security controls, the following measures should be considered:

a) LFIs should maintain an inventory of all its systems and devices, including information such as the networks which they are connected to and their physical locations;

b) Regular enforcement checks to ensure that baseline standards are applied uniformly and non-compliances are detected and raised for investigation;

c) The frequency of enforcement reviews should be commensurate with the risk level of systems;

d) 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.

e) Installing network security devices, such as firewalls, as well as intrusion detection and prevention systems, at critical junctures of 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;

f) 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;

g) Being privy to the risks associated with utilizing WLAN 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;

h) Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced;

i) Information services, users and information systems should be segregated[12] on different network segments on the basis of the purpose for which the system has been established; and

j) Ensuring the security of information in networks and the protection of connected services from unauthorized access. In particular, the following principles must be embraced:

   i. Responsibilities and procedures for the management of networking equipment should be established;

   ii. Operational responsibility for networks should be separated from computer operations where appropriate;

   iii. Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications (include network encryption protocols when connecting to untrusted systems/ networks);

   iv. Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security;

[12] The segregation can be done using either physically different networks or by using different logical networks (e.g. VLAN).

v. Closely coordinate management activities both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

vi. Authenticate all systems on the network; and

vii. Restrict untrusted system connections to the network.

Vulnerability Assessment (VA) and Penetration Testing (PT)

67 VA is the process of identifying and assessing security vulnerabilities in a system. PT can be used to complement the review of security controls and ensure that different facets of the IT system are secured. VA & PT provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). However, PT and VAs are not a substitute for risk assessment.

68 LFIs should conduct VAs regularly to detect security vulnerabilities in the IT environment. To accomplish this, LFIs should:

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

b) Carry out PT in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. Also, PTs on internet-facing systems should be conducted at least annually and full scope penetration tests at least once every two years;

c) Establish a process to remediate the issues identified in VA & PT and perform subsequent validation of the remediation to confirm that gaps are fully addressed;

d) Ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at periodic intervals. The scanning should be either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested;

e) Compare the results and identify repeated vulnerabilities and address either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk; and

f) Ensure that the security function provides status updates regarding the number of unmitigated, critical vulnerabilities, for each department/division, and a plan for mitigating them to senior management on a periodic basis.

Patch Management

69 A patch management process needs to be in place to address technical system and software vulnerabilities quickly and effectively. This will reduce the likelihood of a serious business impact arising from exploitation of newly identified vulnerabilities.

70 LFIs 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, the LFI should establish the implementation timeframe for each category of security patches. Licensees should perform rigorous testing of security patches before deployment into the production environment, since, if not carried out appropriately, it could potentially impact other peripheral systems.

71 The following measures should be considered:

a) Methods should be established to protect information and systems if no patch is available for an identified vulnerability, for example, disabling services and adding additional access controls;

b) Deployment of automated patch management tools and software update tools for all systems for which such tools are available and safe;

c) Measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set; and

d) The patch management process should include:

i. Determining methods of obtaining and validating patches for ensuring that the patch is from an authorized source;
ii. Identifying vulnerabilities that are applicable to applications and systems used by the organization;
iii. Assessing the business impact of implementing patches (or not implementing a particular patch);
iv. Ensuring patches are tested;
v. Describing methods for deploying patches, e.g. automatically;
vi. Reporting on the status of patch deployment across the organization; and
vii. Including methods for dealing with the failed deployment of a patch (e.g., redeployment of the patch).

Security Monitoring

72 Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact their information security and to respond to these events appropriately.

73 As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous monitoring and detection processes should cover:

a) Relevant internal and external factors, including business and information and communications technology ICT administrative functions;
b) Transactions to detect misuse of access by third parties or other entities and internal misuse of access; and
c) Potential internal and external threats.

74 To facilitate prompt detection of unauthorized or malicious activities by internal and external parties, LFIs should establish appropriate security monitoring systems and processes by:

a) 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;

b) 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. LFIs should include capacity management to support business functions, and ensure that indicators such as performance, capacity, and utilization are monitored and reviewed;

c) 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;

d) 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;

e) Regularly reviewing security logs of systems, applications and network devices for anomalies. LFIs should closely supervise staff with elevated system access entitlements and have all their system activities logged and reviewed regularly, as they have the knowledge and resources to circumvent system controls and security procedures;

f) Applying user behavioural analytics in order to enhance the effectiveness of security monitoring. User behavioural analytics can include the use of machine learning algorithms in real time to analyze system logs, establish a baseline of normal user activities and identify suspicious and anomalous behaviours; and

g) Actively monitor technological developments to ensure that they are aware of security risks.

75 The security monitoring process should also help the LFI to understand the nature of operational or security incidents, to identify trends and to support the organization's investigations.

Access Controls

76 Controlling access is essential to protecting system resources against inappropriate or undesired user access. A financial institution must implement an appropriate access controls policy for the identification, authentication and authorization of users (internal and external users such as third party service providers). This must address both logical and physical technology access controls which are commensurate with the level of risk of unauthorized access to its technology systems. Access controls deemed acceptable are as follows:

User Access Management

77 Establishing a user access matrix to outline access rights, user roles or profiles, and the authorizing and approving authorities. The access matrix must be periodically reviewed and updated;

78 Only granting user access to IT systems and networks on a need-to-use basis and within the period when the access is required. Finally, all requests to access IT resources must be duly authorized and approved by the resource owner;

79 Subjecting external employees (such as employees of vendors and service providers) 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;

80 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;

81 Only allowing staff with proper authorization to access confidential information and use system resources solely for legitimate purposes. Additionally, regular reviews of user access privileges should be performed to verify that privileges are granted appropriately and according to the “least privilege” principle. This can assist with the identification of wrongly provisioned, dormant, redundant, toxic or unnecessary access;

82 Enforcing strong password controls over users' access to applications and systems. A financial institution shall periodically review and adapt its password practices to enhance resilience against evolving attacks. This includes the effective and secure generation of passwords and appropriate controls in place to check the strength of the passwords created;

83 Verifying that no person by virtue of rank or position have any intrinsic right to access confidential data, applications, system resources or facilities and ensuring that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities;

84 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;

85 Employing segregation of incompatible functions where no single person is responsible for an entire operation that may provide the ability to independently modify, circumvent, and disable system security features. Therefore, dual control functions should be adopted requiring two or more persons to execute an activity;

86 Employing time-bound access rights which restrict access to a specific period including access rights granted to service providers and limit and control the use of the same user ID for multiple concurrent sessions;

87 Adopting dedicated user domains for selected critical functions, separate from the broader enterprise-wide user authentication system; and

88 Large financial institutions are required to:

a) Deploy an identity access management system to effectively manage and monitor user access to enterprise-wide systems; and
b) Deploy automated audit tools to flag any anomalies.

Privileged Access Management

89 Applying stringent selection criteria and thorough screening when appointing staff to critical operations and security functions, taking into account insider threat. This measure is encouraged since 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. Some common tactics used by insiders to disrupt operations include planting logic bombs, installing stealth scripts and creating system backdoors to gain unauthorized access as well as sniffing and cracking passwords; and

90 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 where possible 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) Restrict vendors and contractors from gaining privileged access to systems without close supervision and monitoring;
j) Protect backup data from unauthorized access; and
k) Ensure privileged user’s activities are in-keeping with the department’s code of conduct.

Online Financial Services

91 LFIs should be cognizant of risks that are brought about as a result of offering their financial services via the internet platform since being an open network, it also brings about security risks that are more sophisticated and dynamic than closed networks and proprietary delivery channels.

92 The degree of risk varies based on the types of services provided over the internet. Typically, financial services offered via the internet can be classified into information service, interactive information exchange service and transactional service. Transactional services pose the highest level of risk as online transactions are often irrevocable once executed. LFIs should clearly identify risks associated with the types of services being offered in the risk management process. Also, they should formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure, for all internet operations.

Online Systems Security

93 In strengthening online systems security, LFIs should:

a) Devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

b) Provide their customers and users of their internet services the assurance that online login access and transactions performed over the internet on their website are adequately protected and authenticated.

c) Properly evaluate the security requirements associated with their internet systems and adopt encryption algorithms, with due regard of the international standards in this area (e.g. PCI-DSS, ISO, NIST).

d) Ensure that information processed, stored or transmitted between the institution and its customers is accurate, reliable and complete. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. Therefore, LFIs should implement physical and logical access security to allow only authorised staff to access its systems. LFIs

should also implement appropriate processing and transmission controls to protect the integrity of systems and data.

e) Implement monitoring or surveillance systems so that it is alerted to any abnormal system activities, transmission errors or unusual online transactions. LFIs should establish a follow-up process to verify that these issues or errors are adequately addressed subsequently.

f) Maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). Measures should be put in place to plan and track capacity utilisation as well as guard against online attacks. These online attacks may include DoS attack and DDoS attack.

g) Implement two-factor authentication at login for all types of online financial systems and transaction-signing for authorising transactions. This secures the customer authentication process and protects the integrity of customer account data and transaction details as well as enhance confidence in online systems by combating cyber-attacks targeted at LFIs and their customers.

h) Perform risk assessments on online financial systems servicing institutional investors, accredited investors or corporate entities, where alternate controls and processes are implemented to authorise transactions. This will ensure that the level of security for these controls and processes, are equivalent or better than using token-based mechanisms to authorise transactions.

i) Take appropriate measures to minimise exposure to other forms of cyber-attacks such as middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

j) Put in place measures to protect customers who use online systems and educate them on security measures that are put in place by the LFI to protect them in an online environment. The LFI should ensure that its customers have access to continual education to raise their security awareness.

k) Not store sensitive internet banking application information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of

the data. Critical web applications should enforce at least TLS 1.2 128 bit encryption level for all online activity.

l) Not re-establish any session after interruption without normal user identification, authentication, and authorisation. Moreover, strong server side validation should be enabled.

Mobile Online Services and Payments Security

94 Mobile Online Services refers to the provision of financial services via mobile devices such as mobile phones or tablets. Customers may choose to access these financial services via web browsers on mobile phones or the LFI's self-developed applications on mobile platforms such as but not limited to Apple's iOS, Google's Android and Microsoft's Windows operating systems. Mobile payment refers to the use of mobile devices to make payments. These payments may be made using various technologies such as near-field communication (NFC).

95 Mobile online services and payments are extensions of the online financial services and payments services which are offered by LFIs and accessible from the internet via computers or laptops. The LFI should implement security measures which are similar to those of online financial and payment systems on the mobile online services and payment systems. LFIs should conduct a risk assessment to identify possible fraud scenarios and put in place appropriate measures to counteract payment fraud via mobile devices.

96 As mobile devices are susceptible to theft and loss, LFIs should ensure that there is adequate protection of sensitive or confidential information used for mobile online services and payments. They should have sensitive or confidential information encrypted to ensure the confidentiality and integrity of these information in storage and transmission. LFIs should perform the processing of sensitive or confidential information in a secure environment.

97 LFIs should educate their customers on security measures to protect their own mobile devices from viruses and other errant software which cause malicious damage and have harmful consequences.

Payment Card Security (ATM, Credit and Debit Cards)

98 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 ATMs or merchants. 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 electronic funds transfer at point of sale (EFTPOS) terminals. LFIs should follow international standards of migrating away from magnetic stripe card types to other, safer, methods (e.g. Europay, MasterCard® and Visa (EMV) chip supported card transactions). Types of payment card fraud include counterfeit, lost/stolen, CNR and CNP fraud. LFIs should monitor payment patterns for insider threat.

Payment Card Fraud

99 In ensuring payment card security:

a) LFIs that provide payment card services should implement adequate safeguards to protect sensitive payment card data. Sensitive payment card data should be 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;

b) Licensees should deploy secure methods to store sensitive payment card data and implement strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (CDA) methods for online and offline card transactions and ensure that magnetic stripes are not used as a means to store sensitive or confidential information for payment cards. For interoperability reasons, where transactions could only be effected by using information from the magnetic stripe on a card, the LFI should ensure that adequate controls are implemented to manage these transactions;

c) Security controls should be implemented at payment card systems and networks;

d) Licensees should only activate new payment cards sent to a customer via post upon obtaining the customer's instruction;

e) A dynamic OTP for CNP transactions via internet should be implemented to reduce fraud risk associated with CNP;

f) Cardholders should be promptly notified via transaction alerts when withdrawals/ charges exceeding customer-defined thresholds are made on customers' payment cards. The transaction alert should include information such as the source and amount of the transaction;

g) Robust fraud detection systems with behavioural scoring or equivalent; and correlation capabilities should be implemented to identify and curb fraudulent activities. Risk management parameters should be set out according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities;

h) Licensees should follow up on transactions exhibiting behaviour which deviates significantly from a cardholder's usual card usage patterns. These transactions should be investigated and the cardholder's authorization should be obtained prior to completing the transaction; and

i) For transactions that customers perform with their ATM cards:

   i. Licensees should only allow online transaction authorization;

   ii. 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

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

ATMs and Payment Kiosks Security

100 ATMSs and payment kiosks have made it convenient for cardholders when withdrawing cash or making payments to billing organizations, however, these systems are vulnerable to card skimming attacks. To better secure these systems, the following counteractive measures can be adopted to boost consumer confidence in the usage of these systems:

a) Install anti-skimming solutions on these machines and kiosks 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 LFI for follow-up response and action;
c) Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission;
d) Implement appropriate measures to prevent shoulder surfing of customers' PINs; and
e) Conduct video surveillance of activities at these machines and kiosks; and maintain the quality of closed-circuit television (CCTV) footage.

101 The LFI should verify that adequate physical security measures are implemented at third party payment kiosks, which accept and process the LFI's payment cards.

IT Audit

102 A financial institution must ensure that the scope, frequency and intensity of technology audits are commensurate with the complexity, sophistication and criticality of technology systems and applications. IT audit provides the BOD 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.

103 IT Audit and Procedures includes the following:
a) Ensuring that audit trails are secured in order to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements;
b) Adequately resourcing the internal audit function with relevant technology audit competencies and sound knowledge of the financial institution's technology processes and operations;
c) Ensuring that internal technology audit staff are professionally certified and adequately conversant with the developing sophistication of the financial institution's technology systems and delivery channels; and

d) Establishing an organizational structure and reporting lines for IT audit in a way that preserves the independence and objectivity of the IT audit function.

Audit Planning and Remediation Tracking

104 An audit plan should provide appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services.

105 Effective programmes are risk-focused, promote sound IT controls, ensure timely resolution of audit deficiencies, and inform the Audit Committee of the effectiveness of risk management practices and internal control systems.

106 Audit Planning and Remediation Tracking measures should include the following:

a) Development of an IT audit plan, comprising auditable IT areas for the next year. The IT audit strategy and plan should be approved by senior management and the licensee's Audit Committee;

b) Establishment of an audit cycle that determines the frequency of IT audits which should be commensurate with the criticality and risk of the IT system or process;

c) A follow-up process to track and monitor IT audit issues and an escalation process should be established to notify the relevant IT and business management of key IT audit issues; and

d) The preparation of an audit summary memorandum by the IT Auditors, which must include an overview of the entire audit process from planning to audit findings, discuss the findings with the auditee and obtain responses. This summary must be done prior to reporting the findings to the Audit Committee. Findings should to be reported and monitored using a systematic audit remediation or compliance tracking methodology.

PART V - REGULATORY PROCESS

Notification for Technology-related Applications

107 LFIs must notify the Bank in accordance with the requirements in paragraphs 108 to 111 prior to conducting e-banking or any other internet services, including introducing new technology relating to e-banking or any other internet services.

108 LFIs offering e-banking or any other internet services for the first time must submit the following information in the notification to the Bank:

a) Risks identified and strategies to manage such risks. This includes specific accountabilities, policies and controls to address risks;
b) Security arrangements and controls;
c) Significant terms and conditions for the services;
d) Client charter on the services;
e) Privacy policy statement; and
f) Any outsourcing or website link arrangements, or strategic alliances or partnerships with third parties that have been finalised.

109 For the introduction of new services, and any enhancements to existing services, the LFI must submit a notification together with the following information:

a) Description of the enhancements to the existing technologies;
b) Risk assessment of the proposed enhancements, including the impact and measures to mitigate identified risks;
c) Assurance from an independent external party that the LFI has addressed the technology risks and security controls associated with the services or any material enhancement to the existing services. The format of the assurance shall be as set out in Appendix 4: Risk assessment Report; and
d) Confirmation by BOD and/or senior management of the LFI's readiness to provide e-banking and/or any other internet services or implement any material enhancement to the e-banking and/or any other internet banking services.

110 LFIs must ensure that the independent external party providing the assurance is competent and has a good track record. The assurance shall address the matters covered in, and comply with *Appendix 5*: *Supervisory Expectations on External Party Assurance*.

111 The LFI may offer the services or implement any enhancement to the services immediately upon submission of the notification under paragraph 107 and compliance with the requirements in paragraphs 108 to 111.

Electronic Reporting Requirements

112 Electronic signature(s) must be legally acceptable and confirm to the criteria set out in the Evidence Act, Chapter 5:03 and Part V of the Electronic Communications and Transactions Bill of 2023.

113 Reporting mechanisms at all times must have the infrastructural capabilities for input and output of data and any necessary reports[13] required by the Bank.

114 Reports generated from a parent company must have policies in place that is above the standards of this guideline and/or equivalent.

115 Non-submission or late submission of reports is a key indicator in the assessment of the risk profile of authorised payment institutions and in deciding which payment institutions need to be inspected.

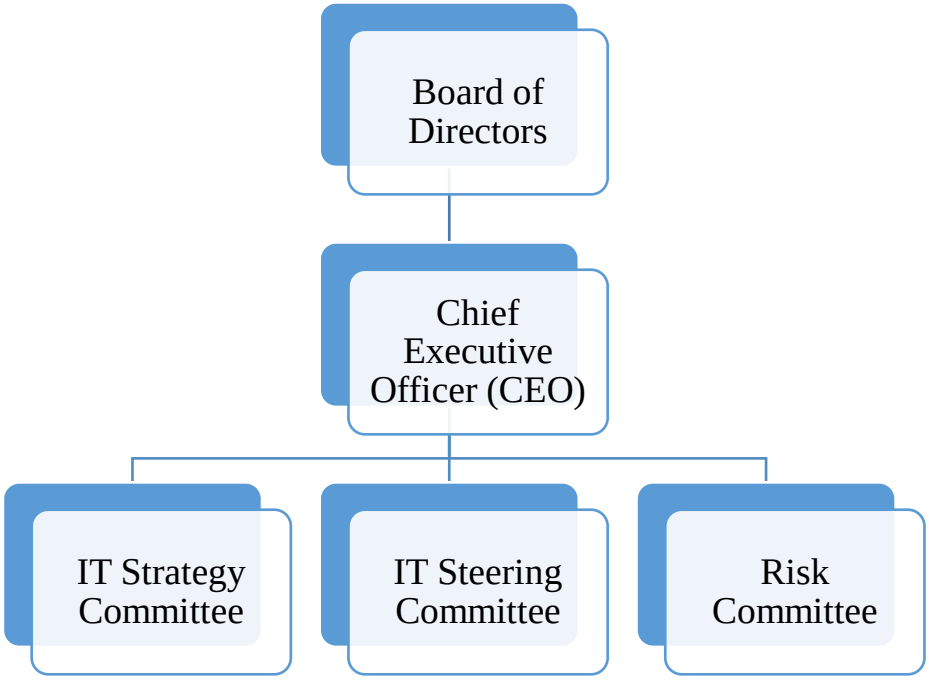
Sanctions

116 When it is established that the institution has failed to comply with this Guideline, the Bank may issue specific directives to that institution and impose any or all the corrective actions under the FIA.

[13] This encompasses reviews, worksheets, schedules and any other document required by the FIA, Supervision Guidelines, Circulars and any other relevant legislation.

PART VI – APPENDICES

APPENDIX 1. PROPOSED IT GOVERNANCE STRUCTURE



**Adapted from the National Bank of Cambodia Technology Risk Management Guidelines*[14].

Diagram 8: IT Governance Structure

[14] The structure is an example. LFIs are expected to adopt a structure commensurate with their risk profile.

APPENDIX 2. TECHNOLOGY RISKS IN FINANCIAL SERVICES

Some of the most significant risks in technology in financial services include[15]:

1. Strategic risk of IT

Examples of risk emanating from IT strategy include:

a) *Embracing versus watching new technology:*

Institutions must balance the risk of adopting new technology against that of ignoring it or waiting for things to settle. Cloud solutions hold both immense promise and significant risk.

b) *Run versus build:*

IT and the business must agree on the appropriate portfolio of investments, specifically on how much to spend to "keep the lights on" versus investing in new technology and capabilities. Overspending on maintenance can crowd out opportunities to adopt new technology and develop new capabilities.

c) *Lack of integration between IT and business strategies:*

Failure to integrate business and IT strategies can lead to inappropriate investments and misaligned expectations. The IT strategy must support evolving business priorities and operating models, and enable agile responses to market developments.

d) *Legacy technology:*

Financial institutions continue to struggle to phase out or decommission outmoded technologies including data centres, platforms and applications. Often technology retained to support select geographies, custom products, or unique processes generate increased complexity and higher costs. When this occurs over hundreds or even thousands of applications, the organization can find itself constrained by its own technology.

[15] Deloitte. Information technology risks in financial services. What board members need to know - and do. https://www.academia.edu/29293320/Information_technology_risks_in_financial_services_What_board_members_need_to_know_and_do

e) *Avoidance of hard truths:*

Mergers and acquisitions multiply applications in technology portfolios when management focuses on short-term cost savings rather than simplifying and upgrading the IT environment. In many cases, bold investments may be required to address years of having avoided expenditures required for a sound and efficient environment.

Questions for the board to pose:

1. What is our organization's IT strategy, particularly as it relates to supporting our businesses, offerings, and customers and other stakeholders?
2. In general, do we as an organization want to be an innovator in IT-enabled financial services or to take the more conservative route and be late adopters? What do we need in place to manage the risks inherent in either strategy?
3. How do we monitor the marketplace for developments that could pose opportunities or risks for our business?
4. What investments are required to remediate and update our legacy IT environment?

2. Cyber security and incident response risk

The many reports of cyber-attacks, data privacy breaches, and misconduct at major companies have pushed cyber security to the top of boards' agendas. Directors need to understand management's view of cyber risks, the potential likelihood and impacts of risk events, and the steps taken to address the risks. It is neither practical nor possible to protect all digital assets equally; in addition to having foundational cyber capabilities across the institution, "crown jewels" should be identified and further protected. Management must be vigilant in identifying emerging threats and implementing effective mechanisms for mitigating them. Moreover, vigilance in cyber security—access controls, security protocols, and the likes should not hinder the ease of doing business objective of institutions.

Cyber incident response (CIR) kicks in when cyber security fails, as it almost certainly will from time to time. The high probability of a cyber-incident dictates that management must have a solid, well-tested CIR plan ready to launch when an incident is detected. Responses should be

proportionate to the incident and cover technical, forensic, communication, and compliance protocols. Priorities might include securing the digital evidence, restoring operations, and notifying senior management, affected stakeholders, and perhaps, law enforcement and regulatory authorities.

Questions for the board to pose:

1. Do we have the right accountability model in place for cyber security? Do we have the right funding and talent?
2. Have we identified our "crown jewels"? What have we done to protect them?
3. Considering the evolving cyber risk landscape, where are our greatest exposures and what investments are required?
4. For which cyber scenarios do we have controls in place?
5. Have we tested our Cyber Incident Response plan? Are we well-rehearsed?

3. IT resiliency and continuity risk

With technology enabling virtually every activity in financial services, the organization's IT must be resilient from disruptions and outages. An organization should have resiliency standards so that investments in resiliency capabilities go toward the technology that supports its most critical business processes. Recovery testing, especially for critical technology, must be rigorous and verify that recovery plans will work.

Institutions need an end-to-end view of all technology required to support a particular product or process to validate that all components can recover from a disruption. Often times, institutions perform one-off testing of a particular technology application, rather than comprehensively testing all technology required to support an end-to-end process such as clearing or settlement. Finally, institutions relying on third-party providers for critical technology services must understand the third party's resiliency and recovery capabilities as if the technology were owned and operated by the institution.

Questions for the board to pose:

1. Have we defined our critical business processes and identified the technology assets applications, infrastructure, and third parties most essential to supporting them?
2. What scenarios have we planned and tested? Have we planned for extended and/ or rolling technology outages?
3. Do we understand the single points of failure (SPOFs) in our technology environment?
4. Have we experienced any situations where we were unable to respond to a technology outage within our planned time frames? Why did our testing process not identify this weakness?
5. What steps need to be taken to reduce the number and mean time of outages?
6. Are we prepared if multiple systems fail at once and do we know which systems are dependent upon one another?

4. Technology vendor and third-party risk

As arrangements with vendors and service providers, joint venture partners, and other third parties proliferate in financial services, so do the risks. Indeed, third parties' own technology risk can generate operational, financial, reputation, and other risks to the institutions that use their services. A clear understanding of these risks can be obscured by business imperatives and enthusiasm for the relationship, by standard forms of assurance provided by vendors, and by check-the-box due diligence processes.

The financial institution as a whole must develop and implement proper due diligence, contracting, and monitoring procedures for all third parties, including technology vendors engaged by IT. Due diligence must be performed on the third party's reputation, strategic alignment, financial viability, compliance, and other attributes.

In addition, IT must take the lead on assessments of IT capabilities of third parties, whether the third party supports IT or the business. While many institutions have mature capabilities to assess third-party cyber and business continuity risk, they should also understand the effectiveness of the third party's technology management processes. For example, ineffective change management procedures at a third party can increase the risk of a service disruption.

Questions for the board to pose:

1. What are the major IT risks associated with the institution's service providers, business partners, vendors, and other third parties?
2. What is our process for due diligence and subsequent monitoring of third-party IT risks?
3. Do we have adequate oversight of vendors with respect to their resiliency and recovery capabilities?

Ineffective data management at a financial institution can open the way to financial fraud, accounting and regulatory reporting issues, and loss of stakeholders' trust. Regulatory agencies are expressing strong interest in data management capabilities, given that risk and capital management depend on reliable, accurate, and timely data. In addition, financial institutions are increasingly combining external data with internal data, adding new layers of complexity to data management and, potentially, new risks.

Rigorous data management capabilities rest on data governance, policy, and procedures that support accuracy, reliability, and timeliness of data, and clarify data ownership, uses and alteration. Controlled creation, transformation, storage, and disposal of data are central to the concept of data integrity.

When institutions retain unnecessary data, they face additional cost, complexity, and risk that it could be breached. Institutions should have policy and standards supporting the sound disposal of data, and assurance that policy is being put into practice.

Questions for the board to pose:

1. How effective are our data management policy and standards?
2. Are critical data elements identified in key applications?
3. How data quality is measured in key services and associated applications?
4. How is data governance integrated with IT processes such as the systems development lifecycle, architecture reviews, and the like?

6. IT program execution risk

At any given time, a large financial institution will have multiple IT programs in development across organizational functions and geographic regions. Examples include enterprise resource planning (ERP), enterprise risk management (ERM), and customer relationship management (CRM) systems. These programs present risks, such as budget overruns, delays, and failure to deliver targeted business results. Generators of risk include programs misaligned with strategic

objectives, program charters that fail to address risks, lack of program governance, uneven execution, misallocation of resources, and lack of formal communication. IT program management is also critical to the success of any merger or acquisition that will combine IT systems.

Management needs to focus on the change management, as well as the technical, aspects of a project and minimize optimistic assumptions in project plans. Use of analytics to identify and manage risks, forecast project outcomes, and identify course corrections as projects unfold is an emerging approach. Data-driven decision making methods can supplement or replace the anecdote-driven approach that often prevails in project planning. Testing the waters with a pilot project can reveal how analytics might work and whether to implement that approach on a broader scale.

Questions for the board to pose:

1. What key IT programs (purchases, projects, implementations) do we now have under consideration or underway?
2. Does our program management framework embed a consistent set of governance processes and tools across the program and flag risks of project delays, budget overruns, and delivery failures early so they can be addressed?
3. Does our IT program coordinate strategic objectives, business processes, and system development over multiyear time frames? How rigorous are we in our planning, communication, and controlling efforts?
4. Have we considered the use of analytics to manage and coordinate our IT programs?

7. Technology operations risk

Management should ensure that rigorous operational processes are in place to protect the integrity of the technology environment. IT needs to deliver services at levels agreed upon with the business, manage capacity, understand and manage its assets, comply with software license agreements, and effectively manage incidents and problems. Non-standard and complex architectures can hinder the ability to meet service performance objectives. A weak incident management process leads to untimely and inconsistent resolution of issues, and missed opportunities to strengthen processes.

Technology environments are not static but are continually evolving. One of the most significant risks is the release of a change into the environment that renders a technology unusable. Management must ensure changes to technology are tested and released appropriately, and handled with great care.

Questions for the board to pose:

1. How many technology changes caused an outage when released or needed to be reversed/rolled back? Which aspects of our current process enabled this situation?
2. In what areas do we lack adequate service level agreements between technology and the business, and, therefore, risk disconnect between service expectations and performance?
3. What are our uptime/downtime statistics for our critical technologies? How could we improve our performance?

8. Risk of ineffective risk management

Financial institutions traditionally pursue a three lines of defence model to address risk. In the first line of defence, product and process owners, identify and manage risk. The second line, frequently executed by risk and compliance functions, provides a risk management structure and independent oversight of the first line. The third line, usually internal audit, provides independent assurance on the effectiveness of the first two lines of defence to the board and senior management.

Finding the right operating model to enable effective technology risk management presents challenges. The risk function may have the risk management expertise, but lack the knowledge of technology that would enable it to provide sound insights on the IT environment. Conversely, the IT function has the knowledge of technology, but lacks the independence needed to provide an unbiased view of risk.

Considering the importance of technology risk today, organizations need to improve skills development and career paths in technology risk management. In fact, demonstrating skills in both technology and risk management could be an additional criterion for management positions such as the Chief Information Officer (CIO) or Chief Risk Officer (CRO).

Questions for the board to pose:

1. How are we structured to balance the need for technical people who can identify technology risks with the need to be independent and objective?
2. What practices do we have in place to monitor major strategic risks in technology?
3. How can we prevent the risk management function from devolving into a control testing function?
4. Have we created paths to management level positions for those serving in our technology risk management function?

APPENDIX 3. INCIDENT MANAGEMENT REPORTING TEMPLATE

Incident Number	
Date & Time Reported	
Function and Site Affected	
Incident Duration (Date & Time)	Date:-
	Time:-
	Duration: -
Incident type/severity (Depending on number of Persons, IT systems, Information Assets Affected) (Tick appropriate option)	Minor ☐ Major ☐ Critical ☐
Business Impact (Number of Branches affected, no. of ATMs, Internet Banking /Customer Service Affected, etc.)	
Whether there is any service level agreement breach? Penalty applicable?	
Incident Reported:	
Root Cause Analysis:	
Corrective action:	
Correction:	
Lessons Learnt:	
Submitted by Head of IT (or equivalent)	
Print Name:	_____
Designation:	_____
Signature:	_____
Date:	_____

APPENDIX 4. RISK ASSESSMENT REPORT

Part A: Financial Institution	
Name of Financial Institution	
Type of Service	New ☐ Enhancement ☐
Description of the Service	
Key contact personnel	
Email Address	
Phone Number	
Part B: External Service Provider	
Name of company	
Engagement period	
Key contact personnel	
Email Address	
Phone Number	
Part C: Detail of application	
Overview of the application, i.e. business case, target segment of demographic and end-user, etc.	*(Maximum 200 words, additional may be provided as supporting documents)*
Description of the technology used to support the product, service or solution.	*(Maximum 200 words, additional may be provided as supporting documents)*
Part D: Technology risk assessment	
Technology risk assessment shall provide assurance on the effectiveness of technology risk control and mitigation performed by the financial institution.	
Part E: Quality Assurance	
Overall Recommendation	
Part F: Authorised signatory	
Name	
Designation	
Signature	
Date	

APPENDIX 5: SUPERVISORY EXPECTATIONS ON EXTERNAL PARTY ASSURANCE

Part A: Financial Institutions are required to provide an external assurance

1. The assurance shall be conducted by an independent external service provider (ESP) engaged by the financial institution.
2. The independent ESP must understand the proposed services, the data flows, system architecture, connectivity as well as its dependencies.
3. The independent ESP shall review the comprehensiveness of the risk assessment performed by the financial institution and validate the adequacy of the control measures implemented or to be implemented.
4. The Risk Assessment Report (as per Part D in Appendix 4) shall state among others, the scope of review, risk assessment methodology, summary of findings and remedial actions (if any).
5. The Risk Assessment Report shall confirm there is no exception noted based on the prescribed risk areas (Negative attestation).
6. The financial institution shall provide the Risk Assessment Report accompanied by the relevant documents.

Part B: Minimum controls to be assessed by the independent External Service Provider, where applicable

1. The independent ESP assessment of security requirements shall include the following key areas:
   a) Access control;
   b) Physical and environmental security;
   c) Operations security;
   d) Communication security;
   e) Information security incident management; and
   f) Information security aspects of business continuity management.
2. For online transactions and services, a financial institution has implemented the following:

a) Adequate measures to authenticate customer identity and ensure legitimate transaction authorisation by the customer, including—

- Measures to prevent session takeover or man-in-the-middle attacks;
- Internal controls must be in place to prevent compromise of relevant internal systems /application /database;
- Where appropriate, apply multi-level authentication, out of band protocol and real-time verification;
- Secure session handling functions and authentication databases; and
- Ensure strong password and cryptographic implementation (recognised algorithm with reasonable key strength).

b) Adequate measures for transaction authentication that promotes non-repudiation and establishes accountability—

- Mechanism exists to ensure proof of origin, content as well as the integrity of the message;
- Chosen channel to deliver transaction is secure;
- Mechanism exists to alert the user on certain type of transactions for further authentication; and
- Establish mutual authentication or appropriate use of digital certification.

c) Segregation of duties and access control privilege for systems, databases and applications—

- Implement dual control where applicable;
- Controls exist to detect and prevent unauthorised access to relevant resources/devices;
- Authorisation database should be tamper-resistant; and
- Periodic review of privileged users.

d) Adequate measures to protect data integrity of transactions and information:

- Implementation of end-to-end encryption for external communication;
- Implementation of multi-layer network security and devices;
- Absence of single point of failures in network architecture;
- Conduct network security assessment/penetration test to identify vulnerabilities;

- Establish audit trail capabilities;
- Preserve the confidentiality of information;
- Use of stronger authentication for higher risk transactions; and
- Timely notification to customers that is sufficiently descriptive of the nature of the transaction.

e) Adequate measures to mitigate associated risks of using electronic mobile devices to perform online transactions, which shall include the following:

- Application is running on secure mobile operating system versions;
- Application is not running on compromised devices;
- Conduct penetration test to identify and rectify potential vulnerability;
- Secure end-to-end communication between the device and host;
- Sensitive information is not stored on mobile devices;
- User is notified of successful transactions;
- User is notified of suspicious transactions;
- Continuous monitoring and takedown of fake applications in application distribution platforms;
- Controls over the uploading of application to application distribution platforms;
- A unique code is generated per transaction; and
- Timely expiry of the transaction code.

Appendix 6 below provides specific guidance regarding more technical areas that should be considered to enhance the security measures of IT systems, networks and infrastructures.

APPENDIX 6. OTHER SECURITY ESSENTIALS

1. Cryptography

The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information and is also commonly used in FIs to protect sensitive customer information such as PINs relating to critical applications (e.g. ATMs, payment cards and online financial systems). Digital signatures/certificates use cryptography as one of the key elements to provide authentication and authorisations.

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information, a robust and resilient cryptography policy must be developed and implemented. This policy, at a minimum, shall address requirements for:

1. The adoption of industry standards for encryption algorithms, message authentication, hash functions, digital signatures and random number generation;
2. The adoption of robust and secure processes in managing cryptographic key lifecycles which include generation, distribution, renewal, usage, storage, recovery, revocation and destruction;
3. The periodic review, at least every three years, of existing cryptographic standards and algorithms in critical systems, external linked or transactional customer-facing applications to prevent exploitation of weakened algorithms or protocols; and
4. The development and testing of compromise-recovery plans in the event of a cryptographic key compromise. This must set out the escalation process, procedures for keys regeneration, interim measures, changes to business-as-usual protocols and containment strategies or options to minimise the impact of a compromise.

When implementing the organisation's cryptographic policy, consideration needs to be given to the regulations and national restrictions that might apply to the use of cryptographic techniques. Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of controls are applied and for what purpose and business processes.

Points to consider

1. Based on a risk assessment, the required level of protection should be identified taking into account the type, strength and quality of the encryption algorithm required;
2. The use of encryption for protection of information transported by mobile or removable media devices or across communication lines should be documented by way of a detailing out of the techniques which can be used at the enterprise level. The policy document should include requirements for managing cryptographic keys through their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys;
3. Cryptographic algorithms, key lengths and usage practices should be selected according to best practice;
4. All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected; and
5. A key management system should be based on an agreed set of standards, procedures and secure methods for:
    - Generating keys for different cryptographic systems and different applications;
    - Issuing and obtaining public key certificates;
    - Distributing keys to intended entities, including how keys should be activated when received;
    - Storing keys, including how authorised users obtain access to keys;
    - Changing or updating keys including rules on when keys should be changed and how this will be done;
    - Dealing with compromised keys;
    - Revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organisation (in which case keys should also be archived);
    - Recovering keys that are lost or corrupted;
    - Backing up or archiving keys;
    - Destroying keys; and
    - Logging and auditing of key management related activities.

2. Remote Access

Employees, vendors, and others are sometimes provided with access to the institution's network and computing resources through external connections. Those connections are typically established through modems, the internet, or private communications lines. Access may be necessary to remotely support the institution's systems or to support the institution's operations at remote locations. In some cases, remote access may be required periodically by vendors to make emergency program fixes or to support a system.

Remote access to LFIs provides an attacker with the opportunity to manipulate and subvert the LFIs' systems from outside the physical security perimeter. Management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices should be strictly controlled.

Points to consider:

1. Restricting remote access by policy and practice unless a compelling business need exists and requiring management approval for remote access.
2. Regularly reviewing remote access approvals and withdrawing those that no longer have a compelling business justification;
3. Functions dealing with critical system processes are normally not allowed through remote access. If the situation so requires, existing controls will need to be re-evaluated or activated when required;
4. Appropriately configuring and securing remote access devices. The LFI should only allow remote access to the LFI's information assets from devices that have been secured, hardened and fully patched according to the LFI's endpoint security standpoint;
5. Performing checks to assess if patches and updates have been applied to remote access devices;
6. Using encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing;
7. Thoroughly testing the remote access infrastructure for vulnerabilities. If cloud infrastructure is used, a review of existing controls, security assessment and security testing should also be conducted to make sure the controls work properly;

8. While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network (VPN) over the Internet to securely communicate data packets over this public infrastructure;
9. Maintaining logs for remote access communications. Logs should include the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access;
10. LFIs need to be aware that using VPNs to allow remote access to their systems can create holes in their security infrastructure. A good practice is to terminate all VPNs to the same end-point in a so called VPN concentrator, and will not accept VPNs directed at other parts of the network;
11. Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based public key infrastructure (PKI)); and
12. Remote access should not be permitted through modems. If it is required, the following steps should be taken:
    - Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorised external requests, and disable the modem immediately when the requested purpose is completed;
    - Configure modems not to answer inbound calls, if modems are for outbound use only; and
    - Use automated call back features so the modems only call one number although this is subject to call forwarding schemes.

3. Wireless Security

The security of wireless networks is a challenge. They do not have well-defined perimeters or well-defined access points. It includes all wireless data communication devices like personal computers, cellular phones, personal digital assistants (PDAs), etc. connected to a LFI's internal networks.

Unlike wired networks, unauthorised monitoring and denial of service attacks can be performed without a physical wire connection and unauthorised devices can potentially connect to the network, perform man-in-the-middle attacks, or connect to other wireless devices. To mitigate

those risks, wireless networks rely on extensive use of encryption to authenticate users and devices and to shield communications. If a LFI uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls.

LFIs deploying WLAN within the organisation should be aware of the risks associated in this environment. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorised access.

Points to consider:

1. Wireless access should only be provided on the basis of strong business case and valid business purpose;
2. Controls should be established to safeguard the confidentiality and integrity of data passing over wireless networks and to protect the connected systems and applications; special controls may also be required to maintain the availability of the network services and computers connected;
3. Wireless networks should be treated as semi trusted networks, and should allow access through authorised devices to shield the internal network from the external risks;
4. Use strong authentication for access point and device identification;
5. Monitor rogue access points and devices trying to connect to wireless networks;
6. LFIs should ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organisations should deny access to those wireless devices that do not have such a configuration and profile;
7. Ensure that all wireless access points are manageable using enterprise management tools;
8. LFIs should use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise;
9. Wireless clients should use strong, multi-factor authentication credentials to mitigate the risk of unauthorised access from compromised credentials; and
10. LFIs should disable wireless peripheral access of devices using Bluetooth.

4. Cloud computing

The computing environment owned by a company is shared with client companies through a web-based service over the Internet which hosts all the programs to run everything from email to word processing to complex data analysis programs. The term cloud computing probably comes from the use of a cloud image to represent the internet or some large networked environment which may include services like software, platform or infrastructure.

However, security and privacy are some of the primary concerns about cloud computing. Corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key. Further, if a client can log in from any location to access data and applications, it's possible the client's privacy could be compromised. Several companies, law firms and universities are debating these and other questions about the nature of cloud computing. Thus, there are issues relating to data security and privacy, compliance and legal/contractual issues. LFIs should be aware of the characteristics of cloud services such as multi-tenancy, data commingling and the higher propensity for processing to be carried out in multiple locations. Hence, LFIs should take active steps to address the risks associated with data access, confidentiality, integrity, sovereignty, recoverability, regulatory compliance and auditing. A few examples of cloud computing risks that need to be managed include the following points.

Points to consider:

1. Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. In particular, LFIs should ensure that the service provider possesses the ability to clearly identify and segregate customer data using strong physical or logical controls. The service provider should have robust access controls in place to protect customer information. Sustainability is also of particular importance to ensure that services will be available and data can be tracked.
2. Enterprises need to seek prior approval from the regulator and confirm to the regulator on the specifics of geographic location of data hosted in the cloud.
3. The cloud provider often takes responsibility for information handling, which is a critical part of the business. Contractual agreement with the cloud service provider should include penalties for failing to perform to the agreed-upon service levels impacting confidentiality, availability and integrity of data.

4. The geographical location of data storage and processing needs to be defined for the cloud data hosting. Trans-border data flows, business continuity requirements, log retention, data retention, audit trails are issues that need to be covered in the contractual agreement.
5. Third-party access to sensitive information creates a risk of compromise to confidential information. It is necessary to ensure the protection of intellectual property (IP), trade secrets and confidential customer information hosted on the cloud.
6. The contractual issues in the cloud services must include coverage related to ownership of intellectual property, unilateral contract termination, vendor lock-in, fixing liability and obligations of cloud service providers, exit clause, etc.
7. Due to the dynamic nature of the cloud, information may not immediately be located in the event of a disaster. Business continuity and disaster recovery plans must be well documented and tested. The cloud provider must understand the role it plays in terms of backups, incident response and recovery. Recovery time objectives should be stated in the contract;
8. The incident management controls for the data hosted in the cloud should be drafted in the contractual agreement with the cloud service provider; and
9. The following points should be addressed from a legal perspective:
    - Whether the user or company subscribing to the cloud computing service owns the data;
    - Whether the cloud computing system, which provides the actual storage space, owns it; and
    - Whether it is possible for a cloud computing company to deny a client access to that client's data.

5. SWIFT Security

SWIFT formally known as the Society for Worldwide Interbank Financial Telecommunication, is a Brussels-based cooperative, maintaining a messaging system used by 11,000 FIs to help move money. The main objective of SWIFT is to ensure authentic, secure and transparent movements of funds across institutions spread over different geographies.

For any organisation operating its own treasury function, and regardless of whether that organisation integrates directly with payment schemes, it is clear that fraudsters are targeting the systems and processes that input into those systems. It is clearly now insufficient to rely on the security of the schemes/LFIs, since the fraudsters are not directly targeting their security. Instead they are targeting insecurity of systems that produce payment instructions in the first place, i.e. LFIs' and corporates' own treasury systems and processes. In order to protect from such risks, LFIs must comply with the latest SWIFT guidelines[16] in order to ensure strict security, confidentiality and integrity protection to the SWIFT environment.

Points to consider:

1. Restrict internet access & segregate critical systems from General IT environment;
2. Reduce attack surface and vulnerabilities;
3. Physically secure the environment to protect access to sensitive equipment, hosting sites, and storage;
4. Prevent compromise of credentials by enforcing passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts;
5. Multi-factor authentication should be used for interactive user access to SWIFT-related applications and operating system accounts;
6. Manage identities and segregate privileges;
7. Detect anomalous activity to systems or transaction records; and
8. Plan for incident response and information sharing

[16] Please refer to the following link to access SWIFT's Customer Security Controls Framework (CSCF): https://www.swift.com/myswift/customer-security-programme-csp

6. Cyber- Attack Exercises

The LFI should carry out regular scenario-based cyber exercises to validate its response and recovery, as well as communication plans in case of a cyber-attack. These exercises could include social engineering[17], table-top[18], cyber range[19], or adversarial attack simulation[20] exercises.

Based on the type and objectives of the exercises, the LFI should involve all relevant stakeholders, inter alia Senior Management, business functions, corporate communications, crisis management team, service providers, and technical staff responsible for cyber threat detection, response and recovery.

The objectives, scope and rules of engagement should be defined before the commencement of the exercise. To ensure that the activities executed don't disrupt the LFI's production system, the exercise must be closely supervised and performed in a controlled environment.

FIs should bear in mind that the simulation of realistic adversarial simulation attacks ought to be designed based on plausible cyber-attacks, and therefore should design the exercises by using threat intelligence that is relevant to their IT environment. This technique facilitates the identification of threat actors who are highly probable to pose a threat to the LFI; as well as to assist in the identification of the tactics, techniques and procedures most likely to be used in such attacks.

---

[17] Social engineering is a process in which cyber criminals manipulate an unsuspecting person into divulging sensitive details such as passwords through the use of techniques such as phishing, identity theft and spam.

[18] A Table-top exercise is a discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

[19] Cyber ranges are interactive, simulative representations of an organization's local network, IT systems, tools, and applications that are connected to a simulated internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and secure environment for product development and security posture testing.

[20] Adversarial attack simulation exercises provides a more realistic picture of an LFI's capability to prevent, detect and respond to real adversaries by simulating the tactics, techniques and procedures of real-world attackers to target people, processes and technology underpinning the LFI's critical business functions or services.