National Bank of Cambodia

Technology Risk Management Guidelines

July 2019

Table of Contents

List of Acronyms **4**

Introduction **5**

1. Information technology governance **6**

1.1. Proposed structure for IT governance 6

1.2. Proposed members for various committees and their roles and responsibilities 6

2. IT governance policy and procedures **7**

2.1. IT policy, standards and procedures 7

3. Information security policy and procedures **9**

3.1. Cyber security essential 9

3.1.1. Access control 9

3.1.2. Network security 11

3.1.3. Remote access 12

3.1.4. Patch management 12

3.1.5. Cryptography controls 13

3.1.6. Vulnerability assessment 14

3.1.7. Physical and environmental security 15

3.1.8. User training and awareness 16

3.1.9. System and Application Security Controls 17

3.1.10. Data Security 18

3.1.11. Wireless security 19

3.1.12. Supplier relationships 20

3.2. Project development and service management 21

3.2.1. Change management 21

3.2.2. Migration controls 22

3.2.3. Incident management 23

3.3. Business continuity considerations 24

3.3.1. Business continuity planning 24

3.4. Audit trails 25

3.5. Technology risk management framework 25

3.5.1. Information security and information asset lifecycle 26

3.5.2. Cyber Risk management 26

3.5. Implementation of new technologies 27

3.5.1. Internet banking 27

3.5.2. Mobile banking and e-wallet 28

3.5.3. Cloud computing 29

3.5.4. SWIFT security 30

3.5.5. Security of ATMs and payment kiosks 30

4. IT services outsourcing 31
4.1. Risk management in outsourcing arrangements 31
4.1.1. Service provider selection 31
5. Information security audit 33
5.1. Audit charter, audit policy to include IS Audit 33
5.2. Planning and IS Audit 33
5.3. Executing an IS Audit 34
5.4. Reporting and follow up 34
5.5. Quality review 34
6. Payment card security 36
6.1. Protecting cardholder data with security standards 36
6.2. Payment card fraud 36
7. Appendix 38
7.1. Executive Stakeholders 38
7.2. Management stakeholders 38
7.3. PDCA 40
7.4. Information asset lifecycle 41
7.4.1. Roles and responsibilities 41
7.4.2. Classification of Information 41
7.5. Incident management reporting template 43

List of Acronyms

BCP	Business Continuity Planning
BFI	Banking and Financial Institution
DDoS	Distributed Denial of Service
DLP	Data Leak Prevention
DoS	Denial of Service
HTML	Hypertext Markup Language
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	System Development Lifecycle
SLA	Service Level Agreement
TLS	Transport Layer Security

Introduction

With Banking and Financial Institutions (BFIs) increasingly using technology to support various business processes, the National Bank of Cambodia (NBC) has established guidelines to help BFIs create a secure technology ecosystem. Implementation of these recommendations needs to be risk based following the stipulations outlined in the guidelines.

The guidelines are primarily expected to enhance the safety, security, and efficiency of BFIs' business operations, which will benefit BFIs and their customers. The progress of implementing these guidelines should be monitored by the top management on an ongoing basis and a review of the implementation status may be put to the Board every year.

The measures suggested for implementation cannot be static. BFIs need to pro-actively create/fine-tune/modify their policies, procedures and technologies based on new developments and emerging concerns.

The NBC will review the progress of implementing these guidelines. The NBC will examine the comprehensiveness and efficacy of the implementation of these guidelines and validate whether they are commensurate with the nature and scope of operations of individual BFIs from 2019.

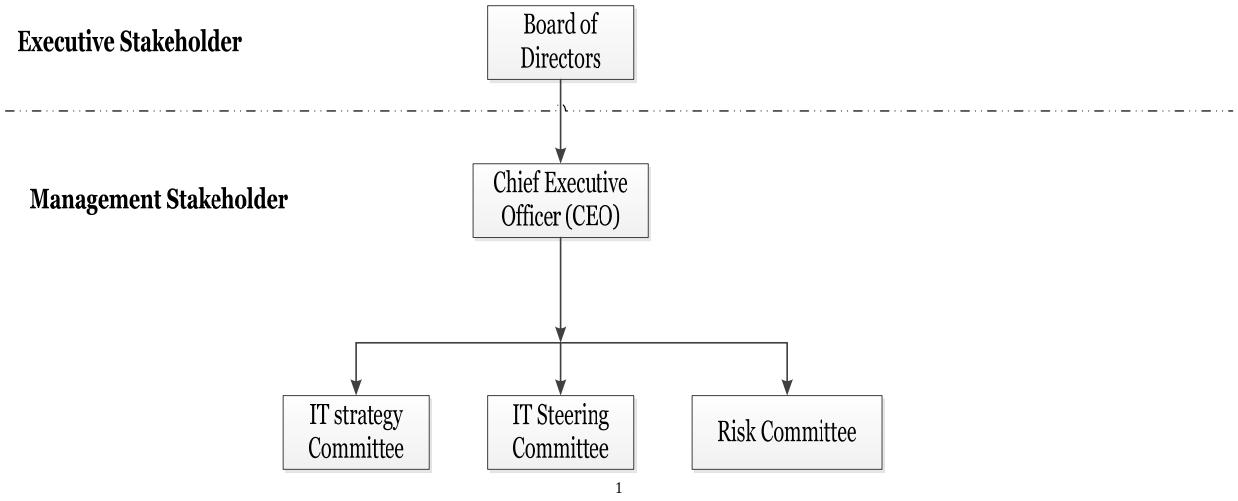
BFIs may have already implemented or may be implementing some or many of the key areas indicated in this guideline. In order to provide a focused project-oriented approach towards implementation of guidelines, BFIs should conduct a formal gap analysis between their current status and suggestion/recommendations as laid out in this guideline and put in place a time-bound action plan to address the gap and in accordance with this guideline. However, BFIs are encourage to implement a basic organisational framework and put in place policies and procedures which do not require extensive budgetary support, infrastructure or technology changes within 3 months after the release of this guideline. The rest of the guidelines should be implemented on voluntary basis within 2 years. The compulsory implementation of this guideline is required upon NBC's notice. Suggestions or recommendations or controls related to technologies/business operations that do not currently exist are left to the discretion of BFIs to implement.

1. Information technology governance

IT governance constitutes the accountability framework of a BFI towards securely operating the technology setup within the organisation. To successfully implement IT Governance, strong support from the Board, well-defined organisation structure, robust processes and continual commitment from the management is required.

The intent of the IT governance structure should be able to adequately support business strategies and aim at achieving organisational objectives.

1.1. Proposed structure for IT governance



[1]

1.2. Proposed members for various committees and their roles and responsibilities

It is important for the organisation to set up robust IT governance structure. IT Governance structure will be of two types, Executive Stakeholders and Management Stakeholders. Examples of the roles and responsibilities of the Executive Stakeholders and Management Stakeholders are given in Appendix 7.1 and 7.2 respectively.

[1] **IT Strategy Committee** members should be: Chief Executive Officer (CEO), Chief Financial Officer (CFO), Other CXO's involved, Information Security Officer. **IT Steering Committee** members should be all Functional Heads.

2. IT governance policy and procedures

The IT policy and procedures should be commensurate with the size, scale and nature of business activities carried out by the BFI. These policies should be the enabling framework for supporting the IT operations.

The broad teams that are typical for a BFI to have within the enterprise IT structure are shown below. The structure is for representation purposes and the BFI may build their own structure. However, the sub-functions within the structure need to be covered as part of the framework created by the BFI.

A. **Enterprise architecture:** Typical roles that are performed by this team include:

a. Defining IT architecture for
   - systems
   - software
   - networks and telecommunications, and
   - other technology interventions

b. Strategic plan
c. Technology lifecycle plan

B. **New product development:** Typical roles that are performed by this team include:

a. Overseeing IT development initiatives or projects
b. Managing budgets & timelines for IT initiatives
c. Ongoing project management
d. Meeting functional expectations
e. Managing outsourced IT teams
f. Ensuring the testing of solutions (developed in-house or outsourced) before going live

C. **IT operations:** Typical roles that are performed by this team include:

a. Set up and oversight of all IT processes involved in managing the technology (such as servers, operating systems, databases, applications and help desks)
b. Infrastructure (such as data centres, networks and telecommunications) thereby ensuring high availability and reliability of systems.

D. **IT compliance:** Typical roles that are performed by this team include all quality, risk and compliance management initiatives within the IT vertical such as performance or conformance metrics, reports, dashboards, internal user feedback and analysis, monitoring IT projects, interaction with audit, risk and compliance functions.

2.1. IT policy, standards and procedures

The IT Governance policy and procedures should cover the following components:

a) Documenting and rollout of IT Operations policy and procedures, and should be approved by the Board
b) Detailed operational procedures should be formulated in relevant areas including for data centre operations
c) IT-related strategy and policy should cover areas such as:
   - IT department's organisational structure[2]
   - Existing hardware and networking architecture
   - Strategy for outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development
   - Strategy for keeping up-to-date with technology developments and systems as and when required
d) BFIs need to follow a structured approach for the short-term and long-term planning process. [3] Short-term and long-term plans should be aligned with the business strategies taking into

[2] An **organisational structure** defines how activities such as task allocation, coordination and supervision are directed toward the achievement of organisational aims

consideration factors such as the organisational model, geographical distribution, technological evolution, legal and regulatory requirements and business vision.

e) There needs to be an annual review of IT strategy and policies taking into account the changes to the organisation's business plans and IT environment.
f) Long-term IT strategy needs to be converted to short-term plans regularly to ensure that the long term goals are achieved.
g) Standards for IT set up such as IT infrastructure baselines (hardening policy) for infrastructure, network architecture and application landscape.
h) Standards for application and system development.
i) Training plan for building internal skills of IT manpower
j) IT compliance guidelines, process for meeting regulatory requirements and operational risk guidelines.
k) IT risk identification framework including identification of risks, tracking of risks and risk mitigation framework.
l) Establish a classification scheme to identify the criticality and sensitivity[4] of enterprise data. The scheme should include factors for identifying critical data and controls for appropriately securing the critical data along with guidelines for data retention and destruction and
m) IT management needs to assess IT risks and suitably mitigate them as necessary.

[3] Considering factors such as organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or market, planning horizon, business process re-engineering, staffing, in- or outsourcing, etc.

[4] Confidential, Internal and Public

3. Information security policy and procedures

A BFI needs to put in place an Information Security Policy that's approved by the Board. The BFI must identify and implement appropriate information security management measures/practices keeping in view their business needs. Given the critical role of technology as part of its business, a BFI needs to subject them to suitable controls across their lifecycle. The controls required to protect the technology set up should include relevant standards and procedures.

The policy needs to be supported with relevant standards, guidelines and procedures. The specified policy should include, but not be limited to the following:

Basic principles of information security

Information security must uphold confidentiality, integrity and availability (known as the CIA triad) as the core principles.

a) **Confidentiality:** prevents the disclosure of information to unauthorised individuals or systems.
b) **Integrity:** means that data cannot be modified without authorisation.
c) **Availability:** for any information system to serve its purpose, the information must be available when it is needed.

Other principles such as authenticity, non-repudiation, identification, authorisation, accountability and auditability are also becoming key considerations for practical security implementations.

a) **Authenticity:** To ensure that the data, transactions, communications or documents (electronic or physical) are genuine, it is important to validate both parties involved are 'who they claim they are'.
b) **Non-repudiation:** Non-repudiation implies one's intention to fulfil one's obligations under a contract/transaction. It also implies that a party to a transaction cannot deny having received or having sent an electronic record. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.
c) **Identification:** Identification is the process by which a subject admits an identity and accountability is initiated. A subject must provide an identity to a system to start the process of authentication, authorisation and accountability.
d) **Authorisation:** Once a subject is authenticated, access must be authorised. The process of authorisation ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity. In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity. If the specific action is allowed, the subject is authorised. Else, the subject is not authorised.
e) **Accountability and auditability:** An organisation's security policy can be properly enforced only if accountability is maintained, i.e., security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities.

3.1. Cyber security essential

The BFIs should secure their IT environment by implementing suitable controls across the IT environment. BFIs are required to consider the following guidelines as part of their Cyber Security policy for protecting the IT environment from Cyber Risk.

3.1.1. Access control

Access control is one of the most critical components for securing technology. Internal sabotage, clandestine espionage or internal attacks by trusted employees, contractors and vendors are among the most serious potential risks that a BFI faces when access control is not effective.

Various factors that need to be considered when authorising access to users and information assets, inter-alia, include business role, physical location, method of connectivity, time of access, and nature of device used to connect.

The governance processes need to include clearly defined controls around the creation, modification, update, change, and revocation of access rights based on business needs. The processes are applicable to both users as well as IT assets connecting with each other.

Role-based access control is an approach used successfully by many organisations to link access rights with business roles.

Points to consider

a) An access control policy needs to established, documented and reviewed based on business and information security requirements. Asset owners needs to determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls, reflecting the associated information security risks.
b) Access controls are both logical and physical and these need to be considered together. Users and asset owners need to be given a clear statement of the business requirements to be met by the access control matrix.
c) The access control matrix should be supported by formal procedures and defined responsibilities. A formal user registration, de-registration and provisioning process needs to be implemented to enable the assignment of access rights. Asset owners should review users' access rights at regular intervals.
d) Among the important controls that need to be considered are:
    - A systematic process of applying and authorising the creation of user IDs and the access control matrix
    - Conducting a risk assessment and granting access rights based on the same.
    - Implementation of role-based access control designed to ensure effective segregation of duties
    - Changing default user names and/or passwords of systems and prohibiting sharing of user IDs and passwords of generic accounts
    - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment/contract
    - Processes to notify in a timely manner the information security function regarding user additions, deletions and role changes
    - Periodic reconciliation of user IDs in a system and actual users required to have access and deletion of any unnecessary IDs, if any
    - Auditing, logging and monitoring of access to IT assets by all users and
    - Considering de-activating user IDs of users of critical applications who are on prolonged leave
e) Segregation should be maintained between those initiating data/transaction (including web page content) and those responsible for verifying the transaction. Further, segregation should be maintained between those developing and those administering systems.
f) For accountability purpose, ensure that users and IT assets are uniquely identified and their actions are auditable.
g) Transaction processes and systems should be designed to ensure that no single employee/outsourced service provider could enter, authorise and complete a transaction.
h) System administrators, security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on the financial systems they maintain or operate by virtue of their job functions and privileged access. Personnel with elevated system access entitlements should be closely supervised with all their systems activities logged, as they have inside knowledge and the resources to circumvent systems controls and security procedures. Some of the control and security practices enumerated below need to be considered:
    - Implementing two-factor authentication for privileged users
    - Instituting strong controls over remote access by privileged users
    - Restricting the number of privileged users
    - Granting privileged access on a ‘need-to-have’ or ‘need-to-do’ basis

- Maintaining audit logging of system activities performed by privileged users
- Ensuring that privileged users do not have access to systems logs in which their activities are being captured
- Conducting regular audit or management review of the logs
- Prohibiting sharing of privileged IDs and their access codes
- Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring and
- Protecting backup data from unauthorised access

i) BFIs may consider using automated solutions such as Identity Access Management tools from Oracle, CA, Microsoft, SailPoint, etc. to enable effective access control and management of user IDs. Such solutions should also be managed effectively to ensure robust access management.

3.1.2. Network security

To ensure the security of the information assets, securing the network using strong network security controls is important. This needs to be enabled by providing authorised access to the internal network using a combination of technology and process controls.

BFIs need to configure IT systems and devices with security settings that are consistent with the expected level of protection. The BFIs should establish baseline standards to facilitate consistent application of security configurations to network devices within the IT environment. The BFIs should ensure that the frequency of enforcement reviews is commensurate with the risk level of systems.

Points to consider

a) The BFI should install network security devices, such as firewalls, anti-virus/anti-malware software as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure, to protect the network perimeters.
b) BFIs deploying Wireless Local Area Networks (WLAN) within the organisation should be aware of the risks associated with the technology. 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.
c) Controls should be implemented to ensure the security of information in networks and the protection of connected services from unauthorised access. In particular, the following items should be considered:
   - Responsibilities and procedures for the management of networking equipment should be established
   - Operational responsibility for networks should be separated from computer operations where appropriate
   - 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.
   - Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security
   - Management activities should be closely coordinated both to optimise the service to the organisation and to ensure that controls are consistently applied across the information processing infrastructure
   - Systems on the network should be authenticated and
   - Untrusted system connections to the network should be restricted
d) 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.
e) Network services can range from simple unmanaged bandwidth to sophisticated services such as VPN, Voice over IP, VSAT, etc. Security features of network services should be:
   - Technology applied for security of network services, such as authentication, encryption and network connection controls
   - Technical parameters required for secured connection with the network services in accordance with the security and network connection rules and

- Procedures for the network service usage to restrict access to network services or applications, where necessary

f) Information services, users and information systems should be segregated[5] on different network segment on the basis of the purpose for which the system have been established and
g) BFIs needs to conduct regular enforcement checks to ensure that the baseline standards [6]are applied uniformly and non-compliances are detected and raised for investigation.

3.1.3. Remote access

BFIs may sometimes provide employees, vendors, and others 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 BFIs provides an attacker with the opportunity to manipulate and subvert the BFIs' 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

a) Disallowing remote access by policy and practice unless a compelling business need exists and requiring management approval for remote access
b) Regularly reviewing remote access approvals and withdraw those that no longer have a compelling business justification
c) Appropriately configuring and secure remote access devices
d) Perform checks to assess if patches and updates have been applied to remote access devices
e) Use encryption to protect communication channels between the remote access device and the institution to restrict the risks related to network spoofing.
f) While using TCP/IP Internet-based remote access, organisations need to establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure. Further, VLANs', network segments to restrict remote access to authorised network areas and applications within the institution.
g) Maintain 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
h) BFIs 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.
i) Enforce two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI) and
j) 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

3.1.4. Patch management

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 zero day or newly identified vulnerabilities.

[5] The segregation can be done using either physically different networks or by using different logical networks (e.g. VLAN).
[6] A Minimum Security **Baseline Standard** (MSB's) will allow organisations to deploy systems in an efficient and standardised manner.

The standards/procedures for patch management includes a method for defining roles and responsibilities for patch management, determining the importance of systems (e.g., based on the information handled, the business processes supported and the environments in which they are used), recording patches that have been applied (e.g., using an inventory of computer assets including their patch levels).

Points to consider

a) The BFI should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. To implement security patches in a timely manner, the BFI should establish the implementation timeframe for each category of security patches.
b) Critical patches must be evaluated in a test environment before being updated into production on enterprise systems. If such patches break critical business applications on test machines, the organisation must devise other mitigating controls that block exploitation on systems where the patch is difficult to be deployed because of its impact on business functionality.
c) The patch management process should include aspects like:
   - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorised source
   - Identifying vulnerabilities that are applicable to applications and systems used by the organisation
   - Assessing the business impact of implementing patches (or not implementing a particular patch)
   - Ensuring patches are tested
   - Describing methods for deploying patches, e.g. automatically
   - Reporting on the status of patch deployment across the organisation and
   - Including methods for dealing with the failed deployment of a patch (e.g., redeployment of the patch).
d) 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.
e) BFIs should deploy automated patch management tools and software update tools for all systems for which such tools are available and safe and
f) BFIs should measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set.

3.1.5. Cryptography controls

Cryptographic[7] controls can be used to achieve different information security objectives[8];

- **Confidentiality:** encrypting information to protect sensitive or critical information, either stored or transmitted
- **Integrity/authenticity:** using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information
- **Non-repudiation:** using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action and
- **Authentication:** using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources

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 policy on the use of cryptographic controls for protection of information needs to be developed and implemented. 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

[7] The science of coding and decoding messages so as to keep these messages secure. Coding takes place using a key that ideally is known only by the sender and intended recipient of the message.
[8] These definitions are specific to cryptography controls

determine whether a cryptographic control is appropriate, what type of controls are applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximise the benefits and minimise the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

Specialist advice needs to be sought in selecting appropriate cryptographic controls to meet the information security policy objectives.

Points to consider

a) 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
b) 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 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
c) Cryptographic algorithms, key lengths and usage practices should be selected according to best practice
d) Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys
e) 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
f) 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.

3.1.6. Vulnerability assessment

Vulnerability assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. The BFIs should conduct VAs regularly to detect security vulnerabilities in the IT environment.

Penetration testing (PT) and vulnerability assessments 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). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

This type of review requires specialist technical expertise.

Points to consider

a) The BFI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA on a periodic basis. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.
b) The BFI should carry out penetration tests at least annually, in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. Soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer the malicious exploit code and then launch that code against targets of interest. 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. BFIs that do not scan for vulnerabilities and address discovered flaws proactively face a significant likelihood of having their computer systems compromised.
c) The BFI should establish a process to remediate the issues identified in VA & PT and perform subsequent revalidation of the remediation to validate that gaps are fully addressed.
d) The BFIs should ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at periodic intervals either with agents running locally on each end system to analyse the security configuration or with remote scanners that are given administrative rights on the system being tested.
e) BFIs should 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) The security function should provide status updates regarding the number of unmitigated, critical vulnerabilities, for each department/division, and plan for mitigating to senior management on a periodic basis.

3.1.7. Physical and environmental security

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. Conceptually, those physical security risks are mitigated through zone-oriented implementations. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.

The requirements for each zone should be determined through the risk assessment. The risk assessment should include, but is not limited to, threats like dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft/destruction, vibration/earthquake, water, criminals, terrorism, political issues (e.g. strikes, disruptions) and other threats based on the entity's unique geographical location, building configuration, neighbouring environment/entities, etc.

These security controls are applicable to locations where critical information assets are kept, such as the data centre, disaster recovery site, server room, etc.

Points to consider

a) BFIs should deploy the following environmental controls:
   - Secure location of critical assets providing protection from natural and man-made threats
   - Restrict access to sensitive areas like data centres, which also includes detailed procedures for handling access by staff, third party providers and visitors and
   - Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunications, servers), access log reviews, etc.
b) Perimeters of a building or site containing information processing facilities should be physically secure (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorised access with control

mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level.

c) A manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorised personnel only.
d) Physical barriers should, wherever applicable, be built to prevent unauthorised physical access and environmental contamination.
e) All fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner.
f) Suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms.
g) The date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorised purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means.
h) Access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card.
i) A physical log book or electronic audit trail of all access should be securely maintained and monitored.
j) All employees, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification.
k) External party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorised and monitored.
l) Access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.
m) Where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities.
n) Physical protection against natural disasters, malicious attack or accidents should be designed and applied.
o) Procedures for working in secure areas should be designed and applied.
    - Personnel should only be aware of the existence of, or activities within, a secure area on a need to-know basis.
    - Unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities.
    - Vacant secure areas should be physically locked and periodically reviewed and
    - Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorised.
p) There should be secure storage of media. Controls could include physical and environmental controls such as fire and flood protection, limiting access by means of physical locks, keypad, passwords, biometrics, etc., labelling, and logged access. Management should establish access controls to limit access to media, while ensuring that all employees have authorisation to access the minimum data required to perform their responsibilities.

3.1.8. User training and awareness

There is a vital need for an initial and ongoing training and information security awareness programme. The programme may be periodically updated keeping in view changes in information security, threats/ vulnerabilities and/or the BFI's information security framework.

All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.

An information security awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for information security and the means by which those responsibilities are discharged. The awareness programme should be planned taking into consideration the employees' roles in the organisation, and, where relevant, the organisation's

expectation of the awareness of contractors. The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors.

Points to consider

a) Awareness training should be conducted for the organisation's personnel covering IT policy, processes and procedures.
b) The organisation should ensure that all personnel who are assigned responsibilities within Information Security Management are trained to perform the required tasks by:
   - determining the necessary competencies for personnel
   - training them for the required competencies, and
   - evaluating the effectiveness of the training.
c) Maintaining records of education, training, skills, experience and qualifications.
d) The organisation should ensure that relevant personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the Information Security Management objectives and
e) Some of the areas that could be incorporated as part of the user awareness programme include:
   - The need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts and agreements
   - Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organisation and external parties
   - Relevant information security policies/procedures
   - Acceptable and appropriate usage of IT assets
   - Access controls including standards relating to passwords and other authentication requirements
   - Measures relating to proper email usage and internet usage
   - Physical protection
   - Remote computing and use of mobile devices
   - Safe handling of sensitive data/information
   - Being wary of social engineering attempts to part with confidential details and
   - Prompt reporting of any security incidents and concerns

3.1.9. System and Application Security Controls

BFIs have different types of applications like the core banking system, delivery channels like ATMs, internet Banking, mobile Banking, phone Banking, network operating systems, databases, enterprise resource management (ERP) systems, customer relationship management (CRM) systems, all used for different business purposes. Users (partners, contractors, consultants, employees and temporary employees) usually access several different types of systems throughout their daily tasks, which makes controlling access and providing the necessary level of protection on different data types difficult and full of obstacles. This complexity may result in unforeseen and unidentified holes in the protection of the entire infrastructure including overlapping and contradictory controls, and policy and regulatory noncompliance.

There are well-known information systems security issues associated with application software, whether the software is developed internally or acquired from an external source. Attackers can potentially use many different paths through the application to do harm to the business; hence it is important to have strong application controls embedded in an enterprise.

Points to Consider

a) Each application should have an owner, which will typically be the concerned business function that uses the application.
b) All application systems should to be tested before going live to satisfy business policies/rules of the BFI and regulatory and legal prescriptions/requirements are met.
c) Source code review should be conducted for all critical applications; at a minimum, this should be after every major update (e.g. any software update released by the vendor categorised as major, any update requiring downtime for the application, etc.).

d) The BFI should exercise due diligence in ensuring its applications have appropriate security controls, taking into consideration the type of processes and complexity of services these applications provide in order to ensure that there is a high degree of system and data integrity.
e) Recovery measures, user access and data protection controls, at the minimum, should be implemented for such applications.
f) All application systems should have audit trails including the clear allocation of responsibilities in this regard.
g) There should be documented standards/procedures for administering the application, which are approved by the application owner and kept up-to-date.
h) There should be measures to reduce the risk of theft, fraud, error and unauthorised changes to information through measures like supervision of activities and segregation of duties.
i) Robust System Security Testing, in respect of critical e-Banking systems, needs to incorporate, among other things, specifications relating to information leakage, business logic, authentication, authorisation, input data validation, exception/error handling, session management, cryptography and detailed logging, as relevant. This needs to be carried out at least every year[9] and
j) Restrictions to access should be based on individual business application requirements and in accordance with the defined access control policy. The following should be considered in order to support access restriction requirements:
    - Providing menus to control access to application system functions
    - Controlling which data can be accessed by a particular user
    - Controlling the access rights of users, e.g. read, write, delete and execute
    - Controlling the access rights of other applications
    - Limiting the information contained in outputs and
    - Providing physical or logical access controls for the isolation of sensitive applications, application data, or systems

3.1.10. Data Security

BFIs need to define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.

A data security theory seeks to establish uniform risk-based requirements for the protection of data elements. To ensure that the protection is uniform within and outside of the institution, tools such as data classifications and protection profiles can be used.

Points to consider

a) Policies regarding media handling, disposal, and transit should be implemented. To enable the protection, the data should be classified and mitigation to the risks to data should be in accordance to the data classification. If data classification is not used, the policies should accomplish the same goal as protection profiles, which is to deliver the same degree of residual risk without regard to whether the information is in transit or storage, who is directly controlling the data, or where the storage may be.
b) Sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimise the distribution of sensitive information, including printouts that contain the information.
c) The storage of data in portable devices, such as laptops and PDAs, poses unique problems. In order to mitigate such risk, encryption of sensitive data, host-provided access controls (e.g. Mobile Device Management (MDM) solutions such as Mobile Iron), etc. should be considered.
d) BFIs should have appropriate disposal procedures for both electronic and paper based media. Contracts with third-party disposal firms should address acceptable disposal procedures. For computer media, data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive data like physical destruction, overwriting data, degaussing, etc.
e) BFIs should maintain the security of media while in transit or when shared with third parties.

[9] **OWASP** (**Open Web Application Security Project**) is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications and the 2011 CWE/**SANS Top 25** Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. They are often easy to find, and easy to exploit.

Policies should include contractual requirements that incorporate necessary risk-based controls, restrictions on the carriers used and procedures to verify the identity of couriers and

f) BFIs may encrypt customer account and transaction data sent for printing while it is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.

Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). BFI may consider such solutions, if required, after assessing their potential to improve data security.

DLP solutions provide a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralised management framework. Most DLP solutions include a suite of technologies that facilitate three key objectives:

- Locate and catalogue sensitive information stored throughout the enterprise
- Monitor and control the movement of sensitive information across enterprise networks and
- Monitor and control the movement of sensitive information on end-user systems.

3.1.11. 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, PDAs, etc. connected to a BFI'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 BFI uses a wireless network, it should carefully evaluate the risk and implement appropriate additional controls.

BFIs deploying Wireless Local Area Networks (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

a) Wireless access should only be provided on the basis of strong business case and valid business purpose.
b) 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.
c) 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.
d) Use strong authentication for access point and device identification.
e) Monitor rogue access points and devices trying to connect to wireless networks.
f) BFIs should ensure that each wireless device connected to the network matches an authorised 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.
g) BFIs should ensure that all wireless access points are manageable using enterprise management tools.
h) BFIs should use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise.

i) BFIs should ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection. BFIs should ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.
j) BFIs should ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorised access from compromised credentials and
k) BFIs should disable wireless peripheral access of devices using Bluetooth.

3.1.12. Supplier relationships

BFIs use third-party service providers in a variety of different capacities. It can be an Internet service provider (ISP), application or managed service provider (ASP/MSP), business service provider (BSP) or payment service provider (PSP). These providers may often perform important functions for the BFIs and usually may require access to confidential information, applications and systems.

When enterprises use third parties, they can become a key component in an enterprise's controls and its achievement of related control objectives. Management should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives.

The effectiveness of third-party controls can enhance the ability of an enterprise to achieve its control objectives. Conversely, ineffective third-party controls can weaken the ability of a BFIs to achieve its control objectives. These weaknesses can arise from many sources including gaps in the control environment arising from the outsourcing of services to the third party, poor control design, causing controls to operate ineffectively, lack of knowledge and/or inexperience of personnel responsible for control functions and over-reliance on the third party's controls (when there are no compensating controls within the enterprise).

Points to consider

a) The organisation should identify and mandate information security controls to specifically address supplier risks. These controls should address processes and procedures to be implemented by the organisation and supplier.
b) Identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organisation will allow to access its information.
c) Define a standardised process and lifecycle for managing supplier relationships.
d) Define the types of information access that suppliers will be allowed, and monitor the same.
e) Monitor processes and procedures to check adherence to established information security requirements. This should be performed for all suppliers.
f) Define procedures for handling incidents and contingencies associated with supplier access including responsibilities of both the organisation and suppliers.
g) Procedures should be established to cover recovery and contingency arrangements to ensure the availability of the information or information processing provided by the third party.
h) Awareness training should be conducted for the organisation's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organisation's systems and information.
i) Identify the transition needs that include relevant clauses in the supplier contract to take care of any eventualities.
j) Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organisation and the supplier regarding both parties' obligations to fulfil relevant information security requirements and
k) The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:
    - Description of the information to be provided or accessed and methods of providing or accessing the information.
    - Classification of information according to the organisation's classification scheme.
    - Legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met.
    - Obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing.
    - Rules of acceptable use of information, including unacceptable use if necessary.

- Either explicit list of supplier personnel authorised to access or receive the organisation's information or procedures or conditions for authorisation, and removal of the authorisation, for access to or receipt of the organisation's information by supplier personnel.
- Incident management requirements and procedures (especially notification and collaboration during incident remediation).
- Relevant regulations for sub-contracting, including the controls that need to be implemented.
- Relevant agreement partners, including a contact person for information security issues.
- Screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern.
- Right to audit the supplier processes and controls related to the agreement and
- Obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report.

3.2. Project development and service management

A robust project development and service management is necessary for supporting the IT systems, services and operations, managing changes, incidents as well as ensuring the stability of the IT environment. To achieve such robustness, the BFI should have policy and procedures for change management, migration controls and incident management as outlined.

3.2.1. Change management

A change management process needs to be established, which covers all types of change. For example, upgrades and modifications to applications and software, modifications to business information, emergency 'fixes', and changes to the computers/networks that support the application. The change management process should be documented, and include testing of changes to ensure that they do not compromise on security controls. Changes should be implemented after sign off has been obtained from appropriate authority to ensure they are made securely, and only authorised changes move to the production.

Integrity of data residing in the underlying application which is undergoing a major change should be validated after every major change. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications.

Points to consider

a) BFIs should establish a change management process to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner.
b) The change management process should apply to changes pertaining to system and security configurations, patches for hardware devices and software updates.
c) Prior to deploying changes to the production environment, the BFI should perform a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems.
d) BFIs should develop and document appropriate test plans for the impending change.
e) BFIs should adequately test the impending change and ensure that it is accepted by users prior to the migration of the changed modules to the production system.
f) BFIs should obtain test results with user sign-offs prior to the migration.
g) All changes to the production environment should be approved by personnel delegated with the authority to approve change requests.
h) To minimise risks associated with changes, BFIs should perform backups of affected systems or applications prior to the change. BFIs should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment.
i) BFIs should establish alternative recovery options to address situations where a change does not allow the BFI to revert to a prior status.
j) BFIs should incorporate appropriate controls in case of exception based and emergency changes and

k) Audit and security logs are useful information which facilitates investigations and trouble shooting. The BFI should ensure that the logging facility is enabled to record activities that are performed during the migration process.

3.2.2. Migration controls

Data migration is the process of transferring data between computer storage types or file formats. It is a key consideration for any system implementation, upgrade, or consolidation. Data migration is usually performed programmatically to achieve an automated migration, freeing up human resources from tedious tasks. Data migration occurs for a variety of reasons, including server or storage equipment replacements, maintenance or upgrades, application migration/ upgrade, website consolidation and data centre relocation.

To achieve an effective data migration procedure, data on the old system is mapped to the new system utilising a design for data extraction and data loading. The design relates old data formats to the new system's formats and requirements. Programmatic data migration may involve many phases but it minimally includes data extraction where data is read from the old system and data loading where data is written to the new system. Automated and manual data cleaning is commonly performed in migration to improve data quality, eliminate redundant or obsolete information, and match the requirements of the new system. Data migration phases (design, extraction, cleansing, load, verification) for applications of moderate to high complexity are commonly repeated several times before the new system is deployed.

There needs to be a documented Migration Policy indicating the requirement of roadmap/migration plan/methodology for data migration (which includes verification of completeness, consistency and integrity of the migration activity and pre and post migration activities along with responsibilities and timelines for completion of same). Explicit sign offs from users/application owners need to be obtained after each stage of migration and after complete migration process. Audit trails need to be available to document the conversion, including data mappings and transformations.

Points to consider

a) The key aspects that are required to be considered include:
   - **Completeness**— ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same).
   - **Availability of data backup**— ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process.
   - **Integrity of data**— ensuring that the data is not altered manually or electronically during the migration process. If such a need exists, having a documented plan to validate pre and post values for the changed data set should exist.
   - **Consistency of data**— the field/record called for from the new application should be consistent with that of the original application and
   - **Continuity**—the new application should be able to continue with newer records (or appendage) and help in ensuring seamless business continuity.

b) A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that:
   - controls in the existing application are not diluted, while migrating data to the new application
   - controls are designed and implemented to meet requirements of an FI's policies and procedures, apart from regulatory and legal requirements, and
   - functionality offered by the application is used to meet appropriate control objectives.

c) A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively.[10]

d) Detailed audit of SDLC process to confirm that security features are incorporated into a new

[10] Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls. This should be coupled with review of underlying environment–operating system, database, middleware, etc.–as weaknesses in the underlying environment can negate the effectiveness of controls at the application layer. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.

system, or while modifying an existing system, should be carried out.

e) A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system should be conducted.
f) The error logs pertaining to the pre-migration/migration/post migration period along with root cause analysis and action taken need to be available for review and
g) After loading into the new system, results should be subjected to data verification to determine whether data was accurately translated, is complete, and supports processes in the new system. During verification, there may be a need for a parallel run of both systems to identify areas of disparity and forestall erroneous data loss. This verification should cover the General Ledger and sub ledger balancing verification in the old and new system.

3.2.3. Incident management

Incident management is defined as the process of developing and maintaining the capability to manage incidents within a BFI so that exposure is contained and recovery achieved within a specified time objective. Incidents can include the misuse of computing assets, information disclosure or events that threaten the continuance of business processes.

BFIs need to have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting to the Board and senior management and customer communication, where appropriate.

Common incident types include, but not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorised access to systems, identity theft, data leakage/loss, malicious software and hardware, failed backup processes, denial of service attacks and data integrity issues.

Points to consider

a) Develop and implement processes for preventing, detecting, analysing and responding to information security incidents.
b) Establish escalation and communication processes and lines of authority.
c) Develop plans to respond to and document information security incidents.
d) Establish the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
e) Develop a process to communicate with internal parties and external organisations (e.g., regulator, media, law enforcement, customers).
f) IT Incidents should be classified into different severity levels based on the business impact and urgency of the incident. The suggested classification levels include:
   - Severity 1 – Incident having high business impact should be reported to the regulator as per the defined frequency in the format provided in Appendix 7.5
   - Severity 2 – Incidents having minimal business impact and
   - Severity 3 – Incidents having no noticeable impact on service delivery or business
g) Integrate information security incident response plans within the organisation's disaster recovery and business continuity plan.
h) Organise, train and equip teams to respond to information security incidents.
i) Periodically test and refine information security incident response plans.
j) Set up vulnerability management process aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide procedures to be carried out should an incident occur.
k) Conduct post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future.
l) Consider incorporating DoS attack considerations in their internet service provider (ISP) selection process and
m) BFIs should consider adopting the PDCA- Plan Do Check Act model to continuously mature and improve their incident management framework. Extract of the model is included in section 7.3.

3.3. Business continuity considerations

The reliability, availability, and recoverability of IT systems, networks and infrastructures plays an important role in maintaining confidence and trust in the operational and functional capabilities of a BFI. When critical systems fail, the disruptive impact on the BFI's operations or customers will usually be severe and widespread and the BFI may suffer serious consequences to its reputation.

3.3.1. Business continuity planning

For the BFI, all the systems are vulnerable. The BFI should define its recovery and business resumption priorities. The BFI should also test and practice its contingency procedures so that disruptions to its business arising from a serious incident may be minimised.

Events that trigger the implementation of a business continuity plan may have significant security implications. Depending on the event, some or all of the elements of the security environment may change. Different trade-offs may exist between availability, integrity, confidentiality, and accountability, with a different appetite for risk on the part of management. Business continuity plans should be reviewed as an integral part of the security process.

Business continuity strategies should consider the different risk environment and the degree of risk mitigation necessary to protect the institution in the event the continuity plans must be implemented. The implementation should consider the training of appropriate personnel in their security roles, and the implementation and updating of technologies and plans for back-up sites and communications networks. These security considerations should be integrated with the testing of business continuity plan implementations.

Points to consider

a) Consider important factors associated with maintaining high system availability, adequate capacity, reliable performance, fast response time, scalability as part of the system design.
b) Identify the critical systems that need to be considered in the BCP plan using a structured approach. This includes conducting Business Impact Analysis and risk assessment.
c) BCP execution team should be established in order to response to any incidence
d) For the identified critical systems ensure that:
    - an adequate management structure is in place to prepare for, mitigate and respond to a disruptive event
    - documented plans, response and recovery procedures are developed and approved, which contains details on how the organisation will manage a disruptive event and will maintain its information security to a predetermined level
    - based on management-approved information security continuity objectives appropriate personnel with the necessary authority, experience and competence are made available to address such events and
    - include incident response personnel with the necessary responsibility, authority and competence to support the continuity plan.
e) Verify their information security management continuity by:
    - exercising and testing the functionality of business continuity processes, procedures and controls to ensure that they are consistent with the business continuity objectives
    - exercising and testing the knowledge and routine to operate business continuity processes, procedures and controls to ensure that their performance is consistent with the business continuity objectives and
    - reviewing the validity and effectiveness of business continuity measures when information systems, information security processes, procedures and controls or business continuity management/disaster recovery management processes and solutions change.
f) Install appropriate mechanisms to backup data to meet the RTO- Recovery Time Objective and RPO- Recovery Point Objective requirements as identified through the risk assessment process.
g) Create a robust rollback plan to restore the systems to primary site and
h) Update the business continuity technical procedures and processes in accordance with changes to the IT operations on periodic basis.

3.4. Audit trails

BFIs need to ensure that audit trails exist for IT assets satisfying the BFIs business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. This could include, as applicable, various areas like transaction with financial consequences, the opening, modifications or closing of customer accounts, modifications in sensitive master data, accessing or copying of sensitive data/information; and granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets.

Audit trails should be secured 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.

Audit and security logs are useful information which facilitates investigations and trouble shooting.

Points to consider

a) Ensure that records of user access are uniquely identified and logged for audit and review purposes.
b) Have accountability and identification of unauthorised access is documented.
c) Enable audit logging of system activities performed by privileged users.
d) Protect against unauthorised changes to log information by using appropriate logging facility. The operational control should include protection from:
    - alterations to the message types that are recorded
    - log files being edited or deleted and
    - storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
e) Ensure that NTP- Network Time Protocol server is used to time sync all internal devices.
f) Ensure appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.
g) Ensure event logs include, when relevant:
    - User IDs
    - System activities
    - Dates, time and details of key events, e.g. log-on and log-off
    - Device identity or location if possible and system identifier
    - Records of successful and rejected system access attempts
    - Records of successful and rejected data and other resource access attempts
    - Changes to system configuration
    - Use of privileges
    - Use of system utilities and applications
    - Files accessed and the kind of access
    - Network addresses and protocols
    - Alarms raised by the access control system and
    - Records of transactions executed by users in applications and online customer transaction
j) Ensure event logging sets the foundation for automated monitoring systems which are capable of generating consolidated reports and alerts on system security.

3.5. Technology risk management framework

The BFI should develop policy and procedures to protect the information assets throughout the lifecycle. Criticality of information system assets should be identified and ascertained in order to develop appropriate plans to protect them. The BFIs should have effective risk management practices and internal controls to achieve data confidentiality[11], system security, reliability, resiliency and recoverability in the organisation.

[11] Data confidentiality refers to the protection of sensitive or confidential information such as customer data from unauthorized access, disclosure, etc.

3.5.1. Information security and information asset lifecycle

Information security needs to be considered at all stages of an information asset's[12] lifecycle like planning, design, acquisition, classification, implementation, maintenance and disposal.

Points to consider

a) Planning and design level controls need to be in place to ensure that information security is embodied in the overall information systems architecture and the implemented solutions are in compliance with the information security policies and requirements of a BFI.
b) Acquisition of new assets and all existing assets should be inventoried. Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health and safety, insurance or financial (asset management) reasons. The inventory record of each information asset should, at least, include:
    - a clear and distinct identification of the asset
    - relative value to the organisation
    - location
    - security/risk classification
    - asset group (where the asset forms part of a larger information system)
    - owner and
    - designated custodian
c) Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules/requirements for each class, it is possible to define the level of access controls that should be applied to each information asset. Classification of information reduces the risk and cost of over- or under- protecting information resources in aligning security with business objectives since it helps to build and maintain a consistent and uniform perspective of the security requirements for information assets throughout the organisation. The example for classification information is provided in the Appendix 7.4
d) Ongoing support and maintenance controls would be needed to ensure that IT assets continue to meet business objectives. Major controls in this regard include change management controls, configuration management and patch management controls.
e) The BFI should define roles and responsibilities of the personnel who play a vital role throughout the information asset lifecycle. The example of the roles and responsibilities is presented in Appendix 7.4
f) The additional controls to protect the information assets should include, but not limited to
    - service level management
    - vendor management
    - capacity management and
    - configuration management
g) Decommissioning and destruction controls should be defined to ensure that information security is not compromised as IT assets reach the end of their useful life. For example, through archiving strategies and deletion of sensitive information prior to the disposal of IT assets.

3.5.2. Cyber Risk management

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organisations should understand the likelihood that an event will occur and the resulting impact. With this information, organisations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

With an understanding of risk tolerance, organisations can prioritise cyber security activities, enabling organisations to make informed decisions about cyber security expenditures. Implementation of risk management programs offers organisations the ability to quantify and communicate adjustments to their cyber security programs. Organisations may choose to handle risk

[12] According to ISO 27001, information asset is defined as data or other knowledge that has value to an organization. An asset extends beyond physical goods or hardware, and includes software, information, people, and reputation.

in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

Globally, some of the leading cyber security risk assessment frameworks have evolved based on five key principles: identify, detect, protect, respond and recover. These key principles are not intended to take a serial path, or lead to a static desired end state but rather help organisations evolve a dynamic cyber security framework. The below principles largely can support the BFIs in building their cyber security framework.

- **Identify –** Develop the organisational understanding to manage cyber security risk to systems, assets, data, and capabilities.

  The activities in the Identify principle are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions and the related cyber security risks enables an organisation to focus and prioritise its efforts, consistent with its risk management strategy and business needs.

- **Protect –** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect principle supports the ability to limit or contain the impact of a potential cyber security event.

- **Detect –** Develop and implement the appropriate activities to identify the occurrence of a cyber security event. The Detect principle enables timely discovery of cyber security events.

- **Respond –** Develop and implement the appropriate activities to take action regarding a detected cyber security event. The Respond principle supports the ability to contain the impact of a potential cyber security event and

- **Recover –** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. The Recover principle supports timely recovery to normal operations to reduce the impact from a cyber security event.

3.5. Implementation of new technologies

BFIs need to carry out due diligence with regard to new technologies since they can potentially introduce additional risk exposures. BFIs need to authorise the large scale use and deployment in the production environment of technologies that have matured to a state where there is a generally agreed set of industry-accepted controls and robust diligence and testing has been carried out to ascertain the security issues of the technology or where compensating controls are sufficient to prevent significant impact and to comply with the institution's risk appetite and regulatory expectations.

Any new business products introduced along with the underlying information systems need to be assessed as part of a formal product approval process which incorporates, among other things, security related aspects and fulfilment of relevant legal and regulatory prescriptions. BFIs need to develop an authorisation process involving a risk assessment balancing the benefits of the new technology with the risk.

3.5.1. Internet banking

Internet banking services and products can provide significant new opportunities for BFIs. It may allow BFIs to expand their markets for traditional deposit-taking and credit extension activities, and to offer new products and services or strengthen their competitive position in offering existing payment services. In addition, internet banking can reduce operating costs for financial institutions.

BFIs to develop a risk management process rigorous and comprehensive enough to deal with all known risks, and flexible enough to accommodate changes in the type and intensity of risks associated with internet banking. The risk management process can be effective only if it is constantly evolving.

Points to consider

a) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks.
b) BFIs need to evaluate security requirements associated with their internet banking systems and other relevant systems and adopt an encryption solution considering the degree of confidentiality and integrity required.
c) BFIs should only select encryption algorithms which are well established by international standards and which have been subjected to rigorous scrutiny by an international cryptographer community or approved by authoritative professional bodies, reputable security vendors or government agencies.
d) BFIs providing internet banking should be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilisation which could be an indication of a DDoS attack. Consequently, the success of any pre-emptive and reactive actions depends on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.
e) BFIs need to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure emerging vulnerabilities are addressed in a timely manner. This assessment should also be conducted as part of any material change.
f) Internet banking applications should not store sensitive 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.
g) Re-establishment of any session after interruption should require normal user identification, authentication, and authorisation. Moreover, strong server side validation should be enabled.
h) BFIs need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks
i) BFIs need to follow a defence in-depth strategy by applying robust security measures across various technology layers.
j) Authentication practices for internet banking:
    - Authentication methodologies involve two basic 'factors':
        - something the user knows (e.g., password, PIN) and
        - something the user has (e.g., ATM card, smart card).
k) Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber-attack mechanisms like phishing, key logging, spyware/malware and other internet based frauds targeted at FIs and their customers.

3.5.2. Mobile banking and e-wallet

For the BFI and Payment Service Provider, a strong mobile strategy is becoming critical to compete in the changing landscape. Customer and employee expectations are increasingly mobile-first, so BFIs and the payment service provider (PSP) need to address this evolution, to build customer loyalty and revenue streams. Digital wallets allow a user to simply wave or tap their smart phone to complete a transaction. The many benefits to providing customers with mobile banking apps far exceeds the risk; however, it is critical to be armed with the current capabilities that are required to defend and protect the mobile apps from security breaches, resist tampering, and ward off hacking attacks and malware exploits.

As mobile Banking continues to grow, so will the number of exploits, and so development teams will face constant challenges to protect their business from security issues. It is, therefore, critical to factor security into long-term mobile banking app development strategy and align with partners and third party vendors.

Points to consider

a) BFIs and PSPs should set daily transaction and amount limits for usage in case of payments. These limits can be allowed based on approved requests at respective branches only.
b) BFIs and PSPs should implement two-factor authentication for fund transfers and payments initiated for high-value transactions wherever possible.
c) An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.
d) An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.
e) A cooling period needs to be in place. The customer must be informed through email or SMS as and when a new payee is added to the wallet. Each new payee should be authorised by the customer based on an OTP from a second channel which also shows the payee details.
f) A risk based transaction monitoring or surveillance process needs to be considered to monitor fraudulent use of wallets and
g) BFIs and PSPs should also implement appropriate measures to minimise exposure to a man-in-the-middle attack (MITM), man-in-the-browser (MITB) attack or man-in-the-application attack.

3.5.3. 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. A few examples of cloud computing risks that need to be managed include the following points.

Points to consider

a) Enterprises need to be particular in choosing a provider. Reputation, history and sustainability should all be factors to consider. Sustainability is of particular importance to ensure that services will be available and data can be tracked.
b) 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.
c) 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.
d) 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
e) 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.
f) 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.
g) 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.

h) The incident management controls for the data hosted in the cloud should be drafted in the contractual agreement with the cloud service provider and
i) Following points should be addressed from a legal perspective:
   - Whether the user or company subscribing to the cloud computing service own the data
   - Whether the cloud computing system, which provides the actual storage space, own it and
   - Whether it is possible for a cloud computing company to deny a client access to that client's data

3.5.4. 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/BFIs, 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. BFIs' and corporate' own treasury systems and processes. In order to protect from such risks the BFIs should comply with the latest SWIFT guidelines in order to ensure strict security, confidentiality and integrity protection to the SWIFT environment.

Points to consider

a) Restrict internet access & segregate critical systems from General IT environment.
b) Reduce attack surface and vulnerabilities.
c) Physically secure the environment to protect access to sensitive equipment, hosting sites, and storage
d) Prevent compromise of credentials by enforcing passwords with appropriate parameters such as length, complexity, validity, and the number of failed login attempts
e) Multi-factor authentication should be used for interactive user access to SWIFT-related applications and operating system accounts.
f) Manage identities and segregate Privileges
g) Detect anomalous activity to systems or transaction records and
h) Plan for Incident Response and Information Sharing

3.5.5. Security of ATMs and payment kiosks

The presence of ATMs and payment kiosks (e.g. SAM and AXS machines) has provided cardholders with the convenience of withdrawing cash as well as making payments to billing organisations. However, these systems are targets where card skimming attacks are perpetrated.

To secure consumer confidence in using these systems, the BFI should consider putting in place the following measures to counteract fraudsters' attacks on ATMs and payment kiosks.

Points to consider

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 BFI 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 CCTV footage.

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

4. IT services outsourcing

As BFIs augment growth and expand business, there is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives.

'Outsourcing' may be defined as BFIs use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the BFI itself, now or in the future. 'Continuing basis' includes agreements for a limited period.

The benefits of outsourcing include efficiencies in operations, increased ability to acquire and support current technology and tide over the risk of obsolescence, increased time availability for management to focus on key management functions, shorter lead time in delivering services to customers, better quality of services, and stronger controls among others.

Outsourcing has been a constant theme in BFI technology over at least few years, as BFIs have become more technology intensive and the required scale of investment has grown exponentially. Many operations have been outsourced to third party vendors comprising external vendors and specialised subsidiaries. Service providers today may be a technology company or specialist outsourcing manager. This decision to outsource should fit into the institution's overall strategic plan and corporate objectives.

Common areas where BFIs have outsourced functions include:

- Technology Operations and
- BFI Operations (e.g. teleworking, call centres, payment card services, payment gateways, customer verification, etc.)

4.1. Risk management in outsourcing arrangements

4.1.1. Service provider selection

Management should identify functions to be outsourced along with necessary controls. Key considerations while signing the outsourcing agreement should include the following.

Points to Consider

i. Due diligence

In negotiating/renewing an outsourcing arrangement, due diligence should be performed to assess the capability of the technology service provider to comply with obligations in the outsourcing agreement. Due diligence should involve an evaluation of all information about the service provider including qualitative, quantitative, financial, operational and reputational factors.

ii. Maintaining caution lists and scoring for service providers (bureau services)

Where possible the BFIs may obtain independent reviews and market feedback to supplement internal findings. BFIs should ensure that information used for due diligence is current.

iii. Reporting to the regulator

BFIs must report to the regulator, where the scale and nature of functions outsourced are significant, or extensive data sharing is involved across geographic locations as part of technology/process outsourcing and when data pertaining to Cambodian operations are stored/processed abroad.

iv. Multiple service provider relationships

A multiple service provider relationship is where two or more service providers collaborate to deliver an end to end solution to the financial institution. Multiple contracting scenarios are possible:

- One service provider may be designated as the 'Lead Service Provider', to manage the other service providers
- BFIs may independently enter into stand-alone contracts with each service provider.

An institution selects from the above or any other contractual relationship, however, remains responsible for understanding and monitoring the control environment of all service providers that have access to the BFIs systems, records or resources.

5. Information security audit

In the past few years, with the increased adoption of technology by BFIs, the complexities within the IT environment have given rise to considerable technology related risks requiring effective management.

This led the BFIs to implement an Internal Control framework, based on various standards and its own control requirements. As a result, a BFI's management needs assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed.

As a consequence, the nature of the Internal Audit department has undergone a major transformation and IS audits are gaining importance as key processes are automated, or enabled by technology. Hence, there is a need for BFIs to re-assess the IS Audit processes and ensure that IS Audit objectives are effectively met.

The scope of an IS Audit includes:

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures and
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions

5.1. Audit charter, audit policy to include IS Audit

An Audit Charter or Policy is a document that guides and directs activities of an internal audit function. An IS Audit, being integral part of an Internal Audit department, should also be governed by the same charter or policy.

Points to Consider

a) The charter should be documented to contain a clear description of its mandate, purpose, responsibility, authority and accountability of relevant members or officials in respect of the IS Audit (namely the IS Auditors, management and Audit Committee) apart from the operating principles.

b) The IS Auditor will have to determine how to achieve the implementation of the applicable IS Audit standards, using professional judgment.

5.2. Planning and IS Audit

An effective IS Audit programme addresses IT risk exposures throughout a BFIs, including areas of IT management and strategic planning, data centre operations, client or server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, applications used in operations, systems development, and business continuity planning.

Points to Consider

a) A well-planned, properly structured audit programme is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT related risks of every size and complexity.

b) 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.

5.3. Executing an IS Audit

Auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors should obtain evidences, perform test procedures, appropriately document findings, and conclude a report.

An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks. 'Vulnerability assessment' was explained earlier in the document.

Points to Consider

a) The assurance work needs to be performed by appropriately trained and independent information security experts/auditors.
b) The strengths and weaknesses of critical internet based applications, other critical systems and networks needs to be carried out before each initial implementation, and at least annually thereafter.
c) Any findings need to be reported and monitored using a systematic audit remediation or compliance tracking methodology.
d) A BFI needs to regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, making any necessary adjustments to ensure emerging vulnerabilities are addressed in a timely manner.
e) This assessment should also be conducted as part of any material change.
f) Robust performance evaluation processes are needed to provide organisations with feedback on the effectiveness of cyber security policy and technical implementation. A sign of a mature organisation is one that is able to self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems.
g) Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and - assessments of organisational and individual business line security related performance and
h) A BFI should manage the information security risk management framework on an on-going basis as a security programme addressing the control gaps in a systematic way.

5.4. Reporting and follow up

This phase involves reporting audit findings to the Audit Committee.

Points to Consider

a) Before reporting the findings, it is imperative that IS Auditors prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses.

5.5. Quality review

Appropriate levels within the IS Audit function are recommended to assess audit quality by reviewing documentation, ensuring appropriate supervision of IS Audit members and assessing whether IS Audit members have taken due care while performing their duties. This will bring efficiency, control and improve quality of the IS Audit.

Points to Consider

a) Assessment of the IS Audit and assurance standards, guidelines, tools and techniques
b) Assessment of audit methodologies, sampling methodologies and other substantive procedures
c) Assessment of risk-based audit planning and audit project management techniques, including follow-up, compliance, actions taken on repetitive observations, closure timelines and exception management

d) Assessment of evidence collection techniques (e.g. observation, inquiry, inspection, interview, data analysis, etc.) used to gather, protect and preserve audit evidence
e) Assessment of audit quality assurance systems and frameworks and
f) Assessment of reporting and communication techniques (e.g. facilitation, negotiation, conflict resolution, audit report structure, issue writing, management summary, result verification, etc.)

6. Payment card security

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

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

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

6.1. Protecting cardholder data with security standards

There are three ongoing steps for payment card security:

- Assess — identifying cardholder data, taking an inventory of your IT assets and business processes for payment card processing, and analysing them for vulnerabilities that could expose cardholder data.
- Remediate — fixing vulnerabilities and not storing cardholder data unless you need it and
- Report — compiling and submitting required remediation validation records (if applicable), and submitting compliance reports to the acquiring BFI and card brands you do business with.

Key Requirements are listed below:

a) Build and Maintain a Secure Network
   - Install and maintain a firewall configuration to protect cardholder data and
   - Do not use vendor-supplied defaults for system passwords and other security parameters

b) Protect Cardholder Data
   - Protect stored cardholder data and
   - Encrypt transmission of cardholder data across open, public networks

c) Maintain a Vulnerability Management Program
   - Use and regularly update anti-virus software or programs and
   - Develop and maintain secure systems and applications

d) Implement Strong Access Control Measures
   - Restrict access to cardholder data by business need to know
   - Assign a unique ID to each person with computer access and
   - Restrict physical access to cardholder data

e) Regularly monitor and test networks
   - Track and monitor all access to network resources and cardholder data and
   - Regularly test security systems and processes

f) Maintain an Information Security Policy
   - Maintain a policy that addresses information security for all personnel

6.2. Payment card fraud

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

The BFI should deploy secure chips to store sensitive payment card data. The BFI should also implement strong card authentication methods such as dynamic data authentication (DDA) or combined data authentication (CDA) methods for online and offline card transactions. As magnetic

stripe cards are vulnerable to card skimming attacks, the BFI should 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 BFI should ensure that adequate controls are implemented to manage these transactions.

For transactions that customers perform with their ATM cards, the BFI should only allow online transaction authorisation. The BFI 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. The BFI should perform regular security reviews of the infrastructure and processes being used by its service providers.

a) The BFI should ensure that security controls are implemented at payment card systems and networks.

b) The BFI should implement a dynamic one-time-password (OTP) for CNP transactions via internet to reduce fraud risk associated with CNP.

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

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

e) The BFI should follow up on transactions exhibiting behaviour which deviates significantly from a cardholder's usual card usage patterns. The BFI should investigate these transactions and obtain the cardholder's authorisation prior to completing the transaction.

7. Appendix

7.1. Executive Stakeholders

- Proposed Members
- Board of Directors and
- Roles and Responsibilities

Board of Directors: The Board should perform the following functions:

a) Approval of IT Governance Policy and Procedures
b) Ensure that management has put an effective IT Governance process in place
c) Ascertain that management has implemented processes and practices that ensure that the IT function delivers value to the business
d) Ensure IT investments represent a balance of risks and benefits and that budgets are adequate and
e) Continuous improvement programme and effective monitoring of IT Risk.

7.2. Management stakeholders

IT Strategy Committee
a) Head of Operations
b) Head of Finance
c) Chief Information Officer and
d) Other CXOs involved

The committee should perform the following functions:

a) Meet expectations as outlined by the Board from time to time
b) Perform oversight functions over IT Steering Committee activities
c) Validate the alignment of IT Strategy with business requirements/plan
d) Ensure IT organisational structure is defined which will help in meeting the business needs
e) Ensure outside expertise is available to the organisation as and when required and
f) Ensure that adequate investments for IT are available for operations and ongoing IT risk management

It is recommended that the committee should have the following powers:
a) Perform oversight functions over the IT Steering Committee (at a senior management level)
b) Investigate activities within this scope
c) Seek information from any employee
d) Build and maintain extended relationships with partner having specific skills wherever deemed necessary
e) Work in partnership with other Board committees to provide input, review and amend the aligned corporate and IT strategies and
f) Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legislative and regulatory compliance, the ethical use of information and business continuity.

IT Steering Committee

a) Representatives from IT Team
b) Representatives from Legal Team
c) Representatives from HR Team and
d) Representatives from the Business Team

Its role is to assist the Executive Management in implementing IT strategy that has been approved by the Board. It includes prioritisation of IT-enabled investment, reviewing the status of projects (including, resource conflict), monitoring service levels and improvements, IT service delivery and projects.

The committee should focus on implementation. Its functions, among other things, includes:

a) Functional leads as designated by strategy committee members
b) Define project priorities and assessing strategic fit for IT proposals
c) Review IT performance measurement and contribution of IT to businesses
d) Assist in governance, risk and control framework and monitoring key IT Governance processes
e) Advice on infrastructure products and provide direction relating to technology standards and practices, and also ensures that the vulnerability assessments of new technology are performed and
f) Ensure compliance to regulatory and statutory requirements and to verify compliance with technology standards and guidelines

Risk Committee

a) Chief Risk Officer
b) Chief Information Officer/Chief Information Security Officer and
c) Information Security Officer

Risk Management Committee:

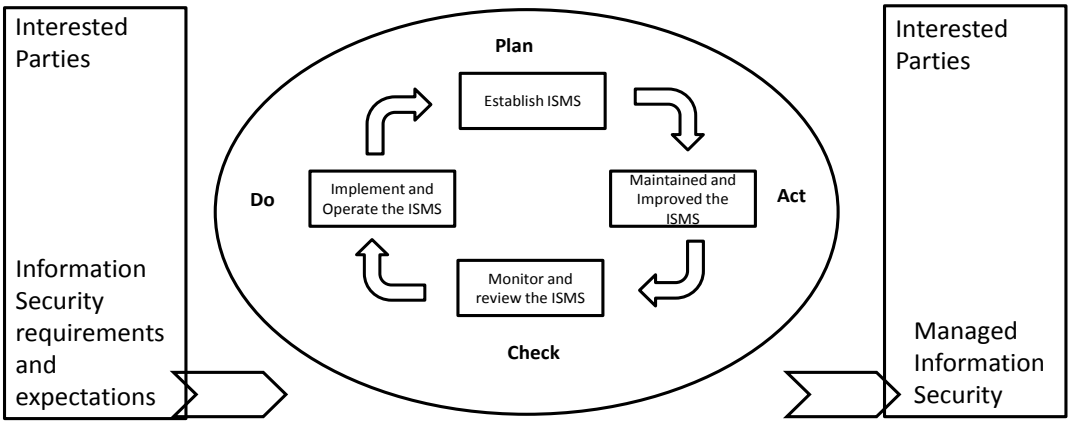
a) Promoting an enterprise risk management competence throughout the FIs, including facilitating development of IT-related enterprise risk management expertise.
b) Effective risk management practices and internal controls should be instituted to achieve data confidentiality, system security, reliability, resiliency and recoverability in the organisation.
c) Establishing a common risk management language that includes measures around likelihood and impact and risk categories, also put in place adequate and robust risk management systems as well as operating procedures to manage the risk.
d) Implementation of appropriate practices and controls to mitigate risks and periodic update and monitoring of risk assessment to include changes in system, environmental or operational conditions that would affect risk analysis and
e) Among executives, the responsibility of the senior executive in charge of IT operations/Chief Information Officer (CIO) is to ensure implementation of policy and processes as defined by the organisation from time to time.

7.3. PDCA

The International Standards have been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security. The adoption of these standards should be a strategic decision for an organisation. The design and implementation of an organisation's information security is influenced by their needs and objectives, security requirements, processes employed and the size and structure of the organisation. It is expected that an information security implementation will be scaled in accordance with the needs of the organisation.

These International Standards adopt the Plan-Do-Check-Act (PDCA) model, which is applied to structure all information security processes. Figure 1 illustrates how an information security takes as input the information security requirements and expectations of the interested parties and through the necessary actions and processes produces information security outcomes that meets those requirements and expectations.

The adoption of the PDCA model will also reflect the principles as set out in the OECD Guidelines (2002)1) governing the security of information systems and networks. This International Standard provides a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.



These and their supporting systems are expected to change over time. It is expected that an information security implementation will be scaled in accordance with the needs of the organisation.[13]

[13] Information Technology Infrastructure Library (ITIL), ISO27001: 2013 Information Security Management System, ISO 22301:2012 Business Continuity Management Systems, ISO 37001:2016 Anti Bribery Management System, Pre-paid Payment Instrument, Payment Card Industry Data Security standard (PCI DSS), National Institute of Standard and Technologies (NIST), Cloud Security Alliance (CSA)

7.4. Information asset lifecycle

7.4.1. Roles and responsibilities

Defining roles and responsibilities must be established and communicated to all relevant personnel and management. Some of the major ones include:

- **Information owner:** This is a business executive or business manager who is responsible for a BFI's business information assets.

- **Information custodian:** The information custodian, usually an information systems official, is the delegate of the information owner with primary responsibilities for dealing with backup and recovery of the business information.

- **Application owner:** The application owner is the manager of the business line who is fully accountable for the performance of the business function served by the application.

- **Security administrator:** Security administrators have the powers to set system-wide security controls or administer user IDs and information resource access rights. These security administrators usually report to the Information Security function and

- **End user:** The end users would be any employees, contractors or vendors of the BFI use information systems resources as part of their job.

7.4.2. Classification of Information

Information classification is defined as the process of assigning an appropriate level of classification to an information asset to ensure it receives an adequate level of protection. The BFIs should consider the following criteria for the classification of information:

- Physical and administrative Controls
- Reproduction of the information
- Distribution of the information and
- Destruction/ Disposal of the information

While BFIs are free to design their own classification schemas, given below are a set of widely accepted classification tiers which can be considered for information classification:

- Private:

  This classification applies to all Personally Identifiable Information (PII), which includes any information that identifies or can be used to identify, contact or locate the person to whom such information pertains.

- Confidential:

  This classification applies to the most sensitive or critical business information, which is intended strictly for use within BFI for exclusive authorized audience. Its unauthorized disclosure could significantly and adversely impact BFI's business, shareholders, business partners, and/or its customers leading to financial, and legal and regulatory repercussions.

- Restricted:

  This classification applies to any sensitive or critical business information which is intended for use within BFI for a limited set of personnel. Its unauthorized disclosure could adversely impact BFI's business, shareholders, business partners, and/or its customers leading to financial repercussions.

- Internal:

  This classification applies to information that is specifically meant for use by BFI employees. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the business, employees, customer, stockholders, and / or business partners.

- Public:

  This classification applies to information, which has been explicitly approved by Public Relations Department for release to the public.

7.5. Incident management reporting template

Incident Number	
Date & Time Reported	
Incident Reported by (Name and Designation)	
Incident Assigned to (Name)	
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 SLA breach? Penalty applicable?	
Incident Reported:	
Root Cause Analysis:	
Corrective action:	
Correction:	
Lessons Learnt:	
Signatures:	

(Incident Handled)	**(Technology Head)**	**(Risk Head)**	**(-NAME-)**
Prepared By: ( )			