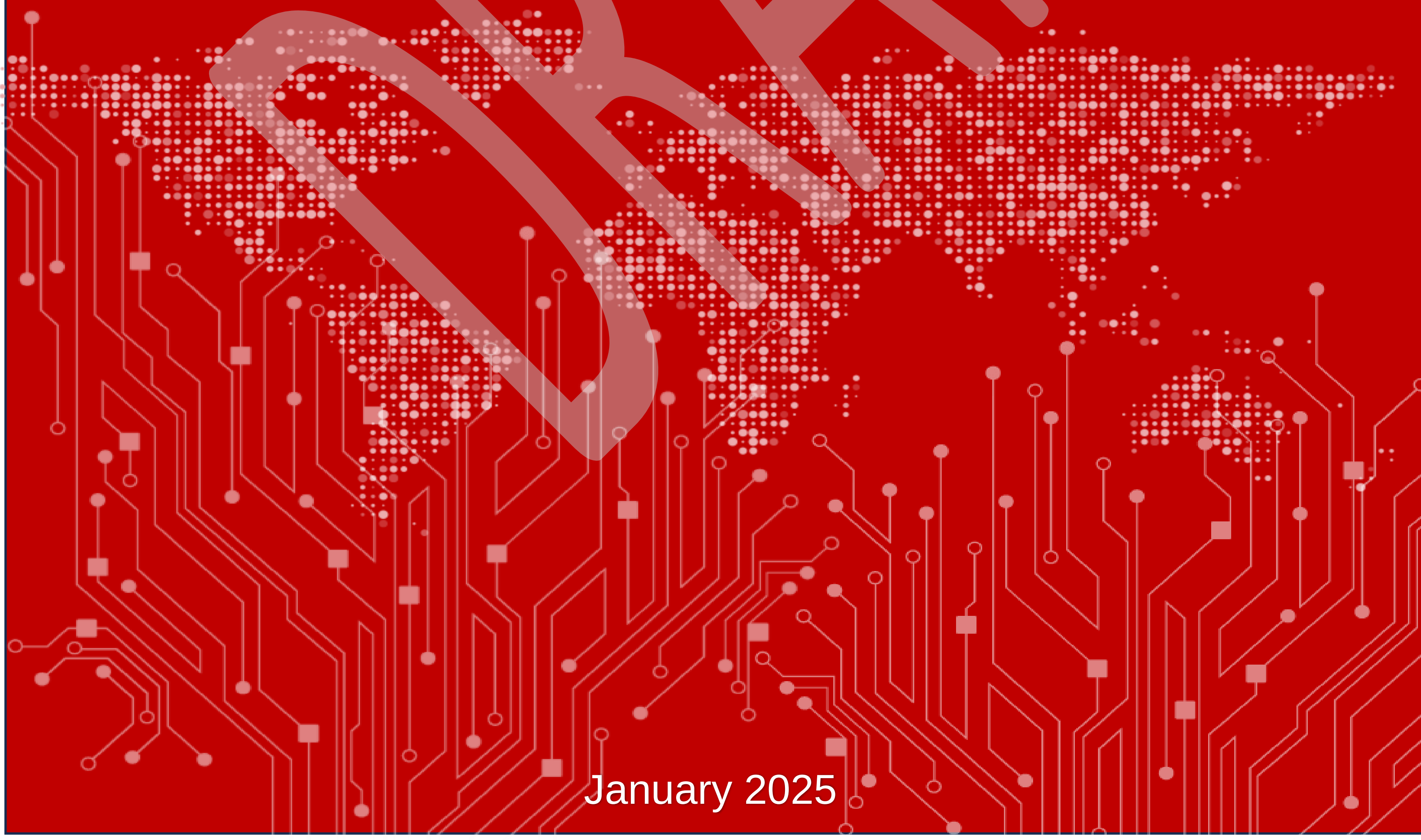
National Bank of Cambodia

Riel Stability Development

Technology and Cyber Risk Management Guidelines



January 2025

Table of Contents

Interpretation

For the purposes of this document, “**Points to consider”** denoted as **Standard (S)** is a requirement that will be assessed for compliance under the guidelines.

Abbreviation

BCM	Business Continuity Management
BCP	Business Continuity Plan
BFIs	Banks and Financial Institutions
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
DDoS	Distributed Denial of Service
DLP	Data Leak Prevention
DoS	Denial of Service
DRP	Disaster Recovery Plan
HTML	Hypertext Markup Language
IEMP	Incident and emergency management plan
KPI	Key Performance Indicators
NBC	National Bank of Cambodia
MTD	Maximum Tolerable Downtime
OTP	One-Time Password
PCI DSS	Payment Card Industry Data Security Standard
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SDLC	Software Development Lifecycle
SLA	Service Level Agreement
SST	Self-service Terminal
TCRMG	Technology and Cyber Risk Management Guidelines
VPN	Virtual Private Network
WAF	Web Application Firewall

Introduction

The Royal Government of Cambodia, in alignment with the national development goals outlined in the Pentagonal Strategy - Phase I, is actively promoting digitalization across various sectors. To support these strategic goals, the Cambodia Digital Economy and Society Policy Framework 2021–2035 was launched with a vision to create a vibrant digital economy and society. This framework aims to lay the foundation for digital adoption and transformation among all social actors, accelerating economic growth and fostering social welfare. Banks and financial institutions (BFIs) are at the forefront of this transformation, leveraging innovative technologies to enhance operational efficiency and customer service.

Despite its significant benefits, digital transformation increases BFIs' exposure to various technology risks, including cyber risks. BFIs must remain vigilant about these risks and establish robust controls to manage them, thereby creating a secure technology ecosystem. To address this need, the National Bank of Cambodia (NBC) introduces the Technology and Cyber Risk Management Guidelines (TCRMG), which supersede the earlier Technology Risk Management Guidelines issued in 2019. The guidelines provide BFIs with principles and best practices for managing risks associated with the use of technology. However, BFIs may utilize additional security best practices if the principles outlined in the guidelines do not adequately support the best interests of BFI's security governance and implementation.

The objectives of the TCRMG are to enable BFIs to:

1. Establish a sound and robust technology risk management framework;
2. Strengthen cyber resilience through continuous improvements in system security, reliability, and resiliency; and
3. Ensure the safety, security, and efficiency of their operations while fostering sustainable growth and protecting customers in the dynamic digital landscape.

The TCRMG outlines principles that address the evolving nature of technology vulnerabilities and cyber threats. They emphasize the importance of implementing a comprehensive risk management framework to safeguard BFIs' systems, protect customer data, and maintain cyber resiliency through proactive defenses against cyber threats.

The implementation of the principles in the guideline should be risk-based, taking into account the nature, size, and complexity of each BFI. BFIs are encouraged to conduct a formal gap analysis between their current practices and the guidelines' principles, and to develop a time-bound action plan to address identified gaps.

By adhering to the guidelines, BFIs can effectively manage technology and cyber risks, thereby creating a safe and secure digital environment. This will support their business operations and contribute to the growth, stability, and sustainability of Cambodia's financial system.

Chapter 1 – Information Technology Governance

1.1 Information Technology Governance Structure

1.1.0 IT governance constitutes a structured framework for ensuring accountability in the secure operation of the organization's technology infrastructure. Effective IT governance hinges on four key pillars: strong board support, well-defined organizational structure, robust processes, and sustained management commitment. Ultimately, a well-designed IT governance framework should seamlessly support with business strategies to facilitate the achievement of organizational objectives. This overarching framework typically includes established functions with clear roles and responsibilities, as well as policies, standards, procedures, guidelines and baselines.

Technology is a key business enabler for BFIs to provide financial services. It is vital that the board and senior management ensure effective internal controls and risk management practices are implemented to achieve security, reliability, and resilience of its operating environment.

BFIs are encouraged to adopt sound corporate governance practices by developing a comprehensive corporate governance policy. This policy should incorporate all relevant laws and regulations governing their operations, and clearly define the roles and responsibilities of the board and committees on existing IT governance. This policy is also a vital tool fostering accountability and transparency.

Points to consider:

1.1.1 (S) It is important for BFIs to set up robust IT governance structure. Examples of the proposed structure are given in **Appendix 2.**

1.1.2 (S) **Foreign bank's branch** may adopt the IT governance structure established by their parent bank or banking group**.**

1.2 IT Organization Structure

1.2.0 As part of the governance structure, BFIs should have an adequate IT structure. Depending on the nature, size, and complexity of each BFI, this structure can take different forms, which includes various teams, departments, systems, processes, and resources that are involved in managing and supporting IT functions such as hardware, software, networks, cybersecurity, data management, and IT services. The broad IT teams typically found within BFIs' structures are designed to ensure the efficient and effective delivery of IT services, support core business operations, and ultimately meet the BFIs' goals and objectives. However, this structure below serves as a reference, and BFIs can tailor it to their specific needs:

a. **Enterprise architecture:** Typical roles performed by this team include defining IT architecture for systems, software, networks, and telecommunications, establishing strategic plans to align IT with business strategies, and meticulously managing the technology lifecycle to optimize resource utilization.
b. **New product development:** Typical roles performed by this team include overseeing IT development initiatives or projects, managing budgets and timelines for IT initiatives, and providing ongoing project management to ensure the meeting of functional expectations. Additionally, they involve managing outsourced IT teams and ensuring the testing of solutions, whether developed in-house or outsourced, before they go live.
c. **IT operations:** Typical roles performed by this team include implementing and overseeing all IT processes related to managing technology components like servers, operating systems, databases, applications, and help desks, as well as overseeing infrastructure elements such as data centers, networks, and telecommunications.
d. **IT compliance:** Typical roles 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, and interaction with audit, risk, and compliance functions.

e. **Information security:** Typical roles performed by this team include designing the information security strategy and program for the BFI. This involves developing information security policies and procedures to safeguard information assets, implementing information security controls, testing security regularly/periodically, and managing information security.

Points to consider:

1.2.1 (S) Depending on the nature, size, and complexity of its business, the BFI shall establish an effective IT function to deliver products and services as well as to provide support day-to-day business operation.

1.2.2 (S) An IT organization structure and description of roles and responsibilities shall be clearly documented and approved by senior management.

1.2.3 (S) The BFI shall establish an equivalent position as Chief Information Technology Officer and Chief Information Security Officer, depending on the nature, size, and complexity of its business.

Chapter 2 – Policies, Standards, and Procedures

2.0.0 The policies, standards and procedures should be commensurate with the nature, size, and complexity of business activities conducted by BFIs. Policies, standards, and procedures should be made available to all staff and supported by appropriate training. To efficiently achieve the objectives of policies and standards as well as consistence level of acceptance across IT infrastructure, BFIs should develop necessary guidelines and baselines.

2.1 IT Operation Policies, Standards, and Procedures

2.1.0 IT operation policy establishes a framework for efficient and effective IT service delivery within BFIs. The policy defines processes for service design, development, deployment, and ongoing support. This policy helps BFIs create a reliable IT environment that supports their goals and delivers exceptional value to users.

Points to consider:

2.1.1 (S) For the effectiveness of IT operations, the BFI shall establish a comprehensive IT operation policy, along with supporting standards and procedures.

2.1.2 (S) The board shall approve the established IT operation policy.

2.1.3 (S) To ensure continued compliance with regulations and best practices, the policy shall be reviewed annually.

2.1.4 (S) Senior management shall approve standards, procedures, guidelines, and baselines. These documents shall be periodically reviewed as needed.

2.1.5 (S) The BFI shall develop an IT-related strategy considering the following areas, but not limited to:

- Department's organizational structure
- Budgeting and resource allocation including capacity building and training
- Existing IT infrastructure and architecture
- Outsourcing, in-sourcing, procuring off-the-shelf software, and in-house development; and
- Keeping up-to-date with technology development and systems when required.

2.1.6 (S) The BFI shall follow a structured approach for the short-term and long-term planning process. Short-term and long-term plans shall be aligned with the business strategies taking into consideration factors such as the organizational model, geographical distribution, technological evolution, legal and regulatory requirements, and business vision.

2.1.7 (S) The BFI shall convert the long-term IT strategy into actionable short-term plans to guarantee progress towards long-term goals.

2.1.8 (S) The IT strategy shall be periodically reviewed, at least once every three years, which considers changes in the BFI's business plans and IT environment.

2.1.9 (S) The BFI shall implement a comprehensive IT compliance framework to ensure adherence to established policies, standards, procedures, regulatory requirements, and operational risk requirements.

2.1.10 (S) The BFI shall develop and execute compliance processes to ensure IT policy, standards and procedures are enforced and to comply with regulatory requirements.

2.2 Information Security Policies, Standards, and Procedures

2.2.0 Information security policies establish a comprehensive framework for protecting BFIs' information assets. The objectives of information security policies are based on confidentiality, integrity, availability, authenticity and nonrepudiation. Other information security principles which are also contributing the safety of critical information assets are identification, authorization, accountability, and auditability.

Points to consider:

2.2.1 (S) The BFI shall establish a comprehensive information security policy along with supporting standards and procedures.

2.2.2 (S) The board shall approve the established information security policy.

2.2.3 (S) To ensure continued compliance with regulations and best practices, the policy shall be reviewed annually.

2.2.4 (S) Senior management shall approve standards, procedures, guidelines, and baselines. These documents shall be periodically reviewed as needed.

2.2.5 (S) The BFI shall develop and execute compliance processes to ensure information security policy, standards and procedures are enforced and to comply with regulatory requirements.

Chapter 3 – IT Operation Management

3.1 Technology Risk Management Framework

3.1.0 Effective technology risk management practices encompass a structured approach to identifying, analyzing, and mitigating risks associated with technology. This involves developing and implementing policies, procedures, and controls to safeguard information assets from potential risks. The objective is to manage risks proactively and to ensure the confidentiality, integrity, availability, and resilience of IT operation environment.

Points to consider:

3.1.1 (S) The BFI shall establish, review, and update their Technology Risk Management Framework (TRMF) periodically to manage technology risks and enhance technology resilience to deal with evolving threat environment. TRMF shall be an integral part of the BFI's enterprise risk management framework.

3.1.2 (S) The framework shall include procedures and processes to identify, assess, manage, monitor, and report on technology risks:

- **Risk identification –** Identify and assess all potential technology risks faced by the BFI;
- **Risk assessment –** Evaluate the likelihood and potential impact of each identified risk to prioritize them based on their severity and the level of threats they pose to the BFI;
- **Risk treatment –** Develop and implement policies, procedures and controls to manage identified risks to an acceptable level based on risk appetite; and
- **Risk monitoring, reviewing, and reporting –** Monitor, review and follow up on technology risks, which include risks that customers are exposed to changes in business strategy, IT systems, environmental or operating conditions, and report key risks to the board and senior management.

3.1.3 (S) The BFI shall ensure that all risks are registered and assigned to the appropriate risk owners who shall be accountable for ensuring that proper risk treatment plans are implemented. Any residual risk arising from threats and vulnerabilities after risk treatment, shall be documented and managed according to the defined risk acceptance criteria that commensurate with the BFI's risk tolerance level.

3.1.4 (S) The BFI shall establish technology risk metrics, which indicate the information assets that have highest risk exposure by taking into account risk events, audit observations, and regulatory requirements.

3.1.5 (S) The BFI shall establish an enterprise risk management function who is responsible for implementing the TRMF at an enterprise-wide level.

3.2 Management of Information Assets

3.2.0 Information assets refer to hardware, software, and data. These assets are not only limited to those owned by BFIs, but also those entrusted to BFIs by customers or third parties, rented or leased by BFIs, and used by service providers to provide services to BFIs.

Points to consider:

3.2.1 (S) The BFI shall establish policy and procedures to protect the information assets throughout the lifecycle.

3.2.2 (S) In planning and design stage, controls shall be implemented in compliance with the information security policies.

3.2.3 (S) Acquisition of new information assets and all existing assets shall be inventoried. The BFI shall keep track of their information assets and periodically update them. Inventories of assets help to ensure that effective protection takes place, and may also be required for other purposes, such as health, safety, insurance, or financial reasons. Inventory records shall categorize information assets into a minimum of three classification types: hardware, software, and data. The following details shall include, but not be limited to:

a. **Hardware asset inventory:** name, description, type, location, serial number, warranty, maintenance plan, asset owner, asset custodian, date of purchase, end of life (EOL) date, manufacturer, vendor, criticality, and sensitivity;
b. **Software asset inventory:** name, description, type, location, license, date of purchase, date of renewal, date of expiration, vendor, asset owner, asset custodian, end of life (EOL) date, criticality, and sensitivity; and
c. **Data asset inventory:** name, description, type, location, classification, retention, business purpose, asset owner, asset custodian, criticality, and sensitivity.

3.2.4 (S) The BFI shall define roles and responsibilities of the staff who have a key role throughout the information asset lifecycle. The example of the roles and responsibilities is shown in **Appendix 3.1**.

3.2.5 (S) Information assets classification has various degrees of sensitivity and criticality in meeting business objectives. The BFI shall assign classes or levels of sensitivity and criticality to information assets and establish specific security rules and requirements for each class to define the level of access controls that shall be applied to each information asset. Classification of information asset lowers the risk and cost of having too much or too little security for information assets by aligning security with business goals, as it helps to create and maintain a consistent and uniform view of the security needs for information assets across the BFI. The example of classes or levels of sensitivity and criticality of information asset can be found in **Appendix 3.2**.

3.2.6 (S) Ongoing support and maintenance controls shall ensure that information assets continue to meet business objectives.

3.2.7 (S) Decommissioning and destruction controls shall be defined to ensure that information security is not compromised even if information assets reach the end of life.

3.3 Configuration Management

3.3.0 Configuration management is an IT service management practice that involves identifying, recording, managing, and updating the configuration items in BFIs' IT infrastructure. Configuration items can consist of hardware components, software applications, network devices, and other resources that support the delivery of IT services. The main objective of configuration management is to manage all configuration items effectively across their lifecycle, allowing BFIs to keep reliable and current information about their IT environment configuration.

Points to consider:

3.3.1 (S) The BFI shall implement a configuration management process to track hardware and software information and ensure effective management of IT environments.

3.3.2 (S) All configuration changes shall be recorded, reviewed, and authorized before they are applied.

3.3.3 (S) The BFI shall conduct acceptance test for any configuration change where there is no acceptance test previously conducted and approved.

3.4 Data Migration

3.4.0 Data migration is the process of transferring data from one storage system or format to another. 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 various reasons, such as changing storage equipment, upgrading applications, or moving data centers. To achieve an effective data migration, BFIs utilize data migration phases (e.g., design, extraction, cleansing, load, and verification). 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.

Points to consider:

3.4.1 (S) The BFI shall develop a data migration policy and procedures that outline the methodology and plan for data migration activities. It includes requirements for verifying the completeness, consistency, and integrity of migration tasks, as well as pre-migration, and post-migration activities and responsibilities.

3.4.2 (S) The BFI shall ensure that data migration procedures addresses, but are not limited to, the following:

- **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** – ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process;
- **Integrity** – ensuring that the data is not altered manually or electronically during the migration process. If necessary, a documented plan to validate pre and post values for the changed data set should exist;
- **Consistency** – the field and record from the new system shall be consistent with that of the original application; and
- **Continuity** – the new system shall be able to operate seamlessly with new records to ensure business continuity.

3.4.3 (S) Explicit sign-offs from users and system owners shall be obtained after each phase of data migration and/or at the completion of the migration process.

3.4.4 (S) Audit trails shall be enabled to document the data conversion, including data mapping and transformation.

3.4.5 (S) A pre-data migration review of system controls, including security features and controls over change management process, shall be performed to confirm that:

- Risk assessment is conducted on data migration;
- Controls in the existing system are not diluted, while migrating data to the new system;
- Controls are designed and implemented in the new system to meet requirements of policies and procedures;
- Functionalities offered by the new system meet appropriate control objectives; and
- Security features are incorporated into the new system, or while modifying an existing system.

3.4.6 (S) During data migration, the BFI shall conduct a review of the control, which include, but are not limited to:

- Monitoring the data migration process;
- Validating configuration and change management process;
- Ensuring a parallel run of both systems to identify areas of disparity and prevent erroneous data loss during a pilot migration before moving to a full data migration; and
- Performing a data migration verification for the pilot data migration and the full data migration, including the general ledger and subledger balancing of the old and new systems.

3.4.7 (S) A post-data migration review of system controls shall be conducted to confirm that:

- The controls as designed are implemented and are operating effectively;
- Any issues or discrepancies identified shall be promptly addressed; and
- A post-data migration audit shall be conducted by the audit function.

3.4.8 (S) The BFI shall ensure that error logs related to the pre-migration, during migration, and post-migration periods are maintained and readily available for review. Root cause analysis shall be conducted on any identified error, and appropriate corrective actions shall be taken to address them effectively.

3.4.9 (S) The BFI shall ensure that the old system data archival and retention periods are in line with relevant laws and regulations and are only accessible with read-only permission if required.

3.5 Patch Management

3.5.0 A patch management process addresses system and software vulnerabilities timely and effectively. This will reduce the likelihood of a serious business impact arising from exploitation of newly identified vulnerabilities and common vulnerability exposure.

Points to consider:

3.5.1 (S) The BFI shall establish patch management policy that includes the identification, categorization, and prioritization of updates and security patches, as well as implementation timeframe for each category.

3.5.2 (S) Patch management procedure shall include, but not be limited to, the following:

- Defining roles and responsibilities for patch management;
- Determining the criticality of systems;
- Specifying turnaround time for deploying patches according to the criticality of patches;
- Determining methods of obtaining and validating patches for ensuring that the patch is from an authorized source;
- Identifying vulnerabilities that are applicable to applications and systems used by the BFI;
- Assessing the business impact of implementing patches or not implementing a particular patch;
- Ensuring patches are successfully tested prior to deployment;
- Describing methods for deploying patches, including failed deployment of a patch (e.g., redeployment of the patch); and
- Reporting on the status of patch deployment across the BFI.

3.5.3 (S) Patches shall be evaluated and tested in a test environment before being updated into production systems. If such patches break critical business applications or their functionality in the test environment, the BFI shall formulate other mitigating controls that block exploitation on systems where the patch is difficult to be deployed.

3.5.4 (S) The BFI shall establish methods to protect information and systems if no patch is available for an identified vulnerability.

3.5.5 (S) The BFI shall deploy automated patch management tools and software update tools for all systems for which such tools are available and safe.

3.5.6 (S) The BFI shall measure the delay in patching new vulnerabilities, and ensure the delay is not beyond the benchmark resolution timeframes.

3.6 Change Management

3.6.0 Change management aims to manage changes in IT environments in order to implement changes correctly, effectively, and securely. An effective change management process helps prevent system and security failures from inadequate controls.

Points to consider:

3.6.1 (S) The BFI shall establish a change management policy and procedures to ensure that changes to production systems are evaluated, authorized, executed, documented, and reviewed in a controlled manner.

3.6.2 (S) The change management procedures shall cover all types of change, which include, but not be limited to:

- Upgrade and modification related to configurations of application, system, and security;
- Patches and updates for hardware and software; and
- Emergency fixes.

3.6.3 (S) Before deploying changes to the production environment, the BFI shall perform a risk and impact analysis of the change request in relation to existing infrastructure, network, upstream and downstream systems.

3.6.4 (S) The BFI shall ensure that all the changes are properly tested. Test plans and test results with user sign-off shall be well documented.

3.6.5 (S) All changes to the production environment shall be approved by personnel delegated with the authority to approve change requests.

3.6.6 (S) To minimize risks associated with changes, the BFI shall perform backups of affected systems or applications before the change. The BFI shall establish a rollback plan to go back to a previous version of the system or application if a problem arises during or after the deployment.

3.6.7 (S) The BFI shall establish alternative recovery options to address situations where a change does not allow BFI to revert to a prior status.

3.6.8 (S) Integrity of data residing in the underlying application which is undergoing a major change shall be validated after every major change.

3.6.9 (S) The BFI shall incorporate appropriate controls in case of exception-based and emergency changes.

3.6.10 (S) Audit and security logs are useful information which facilitates investigations and troubleshooting. The BFI shall ensure that the logs are enabled to record activities that are performed during the migration process from testing to production environment.

3.7 Release Management

3.7.0 Release management involves the controlled process of moving software code and scripts from developing, testing to production environments. This process is critical to ensure that only verified and authorized code is deployed. Unauthorized or malicious code injected during this process could compromise data integrity, system security, and operational processes in the production environment. Therefore, robust controls and thorough testing are essential to mitigate these risks.

points to consider:

3.7.1 (S) The BFI shall establish separate logical environments for software development, testing, staging, and production.

3.7.2 (S) The BFI shall implement segregation of duties to prevent any one individual from having the capability to develop, compile, and transfer object codes between different environments.

3.7.3 (S) The BFI shall ensure controls are implemented to maintain traceability and integrity for all software codes that are moved between IT environments.

3.7.4 (S) After implementing a change successfully in the production environment, the BFI shall replicate the change to the disaster recovery environment.

3.8 Incident Management

3.8.0 Incident management is defined as the process of developing and maintaining the capability to manage incidents within BFIs 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. Common incident types include, but are not limited to, outages/degradation of services due to hardware, software or capacity issues, unauthorized access to systems, identity theft, data leakage and loss, malicious software and hardware, failed backup processes, and denial-of-service attacks.

Points to consider:

3.8.1 (S) The BFI shall establish an incident management policy and procedure to detect, respond to, and mitigate IT incidents, including cyber security incidents.

3.8.2 (S) The incident management framework shall include, but not be limited to, the following:

- Roles and responsibilities of staff who are involved in the incident management process, which covers recording, analyzing, escalating, decision making, resolution, and monitoring incidents;
- Criteria for determining the severity levels of incidents to ensure appropriate prioritization and response;
- Process for incident escalation and resolution threshold to ensure that the time taken to resolve an incident corresponds to its assigned severity level; and
- Communication plan that includes processes and procedures to communicate with internal and external parties (e.g., regulator, media, law enforcement, and customers).

3.8.3 (S) The BFI shall consider adopting the Plan-Do-Check-Act (PDCA) model or other relevant models to continuously mature and improve their incident management framework.

3.8.4 (S) The BFI shall establish incident response plan, including cyber incidents, to quickly contain and mitigate incidents and cyber threats, and to securely and timely resume affected services. The plan shall include communication channels, roles, and responsibilities of relevant internal and external parties to support effective incident response.

3.8.5 (S) The BFI shall test the incident response plan at least annually, incorporating scenario planning and cyber drill exercises with both internal and external parties.

3.8.6 (S) The BFI shall establish an incident respond team and train them to respond to incidents.

3.8.7 (S) Incidents shall be classified into different severity levels based on the business impact and urgency. An example of classification levels is provided in **Appendix 5**.

3.8.8 (S) The BFI shall consider incorporating DoS attack prevention in their internet service provider (ISP) selection process.

3.8.9 (S) The BFI shall report the incident as required by NBC periodically or ad hoc basis.

3.8.10 (S) Post-mortem analysis and review shall be conducted to identify the causes of incidents, develop corrective actions, reassess risks, and adjust controls appropriately to reduce related risks in the future.

3.9 Problem Management

3.9.0 Problem management is a proactive process that identifies, analyzes, and resolves frequent or long-lasting problems within BFIs. Problem management prevents incidents from recurring by dealing with their root causes, whereas incident management concentrates on restoring services as soon as possible after an incident happens.

Points to consider:

3.9.1 (S) The BFI shall establish problem management procedure to include, but not be limited to, the following:

- Roles and responsibilities for staff involved in problem management;
- Process to identify, classify, prioritize, and address problems;
- Root cause analysis of past incidents, which include lessons learnt, to identify and prevent similar or repeated problems;
- Classification of problems based on severity levels to prioritize responses and resource allocation; and
- Monitoring, escalation, and resolution for each problem based on severity levels.

3.9.2 (S) The BFI shall diagnose recurring patterns and commonalities to ensure accurate root cause identification and resolution by conducting periodic analysis of historical incidents.

3.10 Infrastructure Capacity and Performance Management

3.10.0 Infrastructure capacity and performance management enables BFIs to align their IT infrastructure with business needs, maintain high-performance levels, and effectively manage IT resources to support business growth and operational efficiency.

Points to consider:

3.10.1 (S) The BFI shall establish appropriate thresholds and performance metrics that enable monitoring of system performance and reporting of such metrics.

3.10.2 (S) The BFI shall establish a capacity and performance management procedure to include, but not be limited to, the following:

- Roles and responsibilities for personnel engaged in capacity and performance management activities;
- Continuous monitoring of system performance, with timely and detailed reporting of events and exceptions; and
- Regular review and update of capacity and performance management objectives to adapt to changes in technology, business requirements, and regulatory requirements.

3.10.3 The BFI shall establish an infrastructure capacity and performance plan by taking into account future demand and stress test.

3.10.4 The BFI may consider implementing performance management and monitoring tools to monitor an alert when there is over usage or abnormalities of system resources.

3.11 Physical and Environmental Security

3.11.0 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 implementation. Zones are physical areas with differing physical security requirements. The security requirements of each zone are a function of the sensitivity and criticality of the data contained or accessible through the zone, and the information technology components in the zone.

Points to consider:

3.11.1 (S) The BFI shall conduct the risk assessment to identify the security requirements for each zone, where critical information assets are kept, such as data center, disaster recovery site, and server room, etc. The risk assessment shall include, but not be limited to, threats like dust, electrical supply interference, electromagnetic radiation, explosives, fire, smoke, theft, earthquake, flood, criminal, terrorism, political issues (e.g., strikes) and other threats based on the BFI's unique geographical location.

3.11.2 (S) The BFI shall deploy the following environmental controls, including but not limited to:

- Secured location of critical assets providing protection from natural and man-made threats;
- Restricted access to sensitive areas like data centers, 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 related to temperature, water leakage, smoke, access alarms, service availability alerts (for power supplies, telecommunications, and servers), access log reviews, etc.

3.11.3 (S) The perimeters of a building or site with information processing facilities shall be physically secure (i.e., no gaps or weak spots); the roof, walls and floor of the site shall be solid; all exterior doors shall have control mechanisms (e.g., bars, alarms, locks) to prevent unauthorized access; doors and windows shall be locked when not in use; and external protection shall be considered for windows, particularly at ground level.

3.11.4 (S) A reception area or other means of controlling physical access to the site or building shall be in place. Access to sites and buildings shall be restricted to authorized individuals only.

3.11.5 (S) Physical barriers shall, wherever applicable, be built to prevent unauthorized physical access and prevent contamination from the outside environment.

3.11.6 (S) All fire doors on a security perimeter shall 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 shall operate in accordance with the local fire code in a failsafe manner.

3.11.7 (S) The BFI shall install suitable intruder detection in according with national, regional, or international standards and periodically test them to ensure coverage of all external doors and accessible windows. Unoccupied areas shall be enabled with alarm at all times; coverage shall also be provided for other areas, e.g., computer rooms or communication rooms.

3.11.8 (S) All employees, contractors and external parties shall be required to wear some form of visible identification. Unescorted visitors or anyone not wearing visible identification shall be immediately notified to security personnel.

3.11.9 (S) A visitor logbook shall be available and electronic audit trail of all access shall be securely maintained and reviewed on periodically basis.

3.11.10 (S) The date and time of entry and departure of visitors shall be recorded, and all visitors shall be always authenticated and escorted by authorized personnel. They shall only be granted access for specific and authorized purposes with instructions on the security requirements of the area and emergency procedures.

3.11.11 (S) Access to areas where confidential information is processed or stored shall be restricted to only authorized personnel by implementing appropriate access controls, which includes two-factor authentication mechanism.

3.11.12 (S) External support service personnel shall be granted with restricted access to secure areas or confidential information processing facilities only when required. This access should be authorized, and access activities shall be tracked for security purposes.

3.11.13 (S) All physical access rights to secure areas shall be periodically reviewed, updated, and revoked when necessary.

3.11.14 (S) Procedures for working in secure areas shall be designed and applied, which includes, but are not limited to:

- Personnel shall only be aware of the existence of, or activities within, a secure area on a need to-know basis;
- Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities;
- Vacant secure areas shall be physically locked and periodically reviewed; and
- Photographic, video, audio, or other recording equipment, such as mobile devices with built-in camera, shall not be allowed, unless authorized.

3.11.15 (S) Storage of media shall be securely stored with protections like fire and flood safety, and physical locks with passwords or biometrics. Access control shall be implemented to limit access to media with the minimum access required to perform their responsibilities.

3.12 Backup and Recovery Management

3.12.0 Backup and recovery are essential to prevent data loss in case of system disruption. It involves deciding how often and how long to backup, restore, keep and securely destroyed alternative system or data.

Points to consider:

3.12.1 (S) The BFI shall establish and review a backup and recovery policy and procedures to cover the life cycle of backup and recovery process.

3.12.2 (S) The backup and recovery procedures shall include, but not be limited to, backup frequency, retention period, data storage methods, and destruction methods.

3.12.3 (S) The BFI shall periodically test the restoration of system and data backups, including media to validate the effectiveness of its backup and restoration process.

3.12.4 (S) The BFI shall protect any confidential data in backup media from unauthorized access and modification. Backup media shall be kept at a secure separate location.

3.13 Data Center Resiliency

3.13.0 Data center resiliency is the ability of a data center facility to maintain its critical operations and services under various disruptions, including power outage, equipment failure, natural disaster, cyberattack, and human error. It involves implementing redundant systems, robust infrastructure, and proactive measures to ensure high availability, fault tolerance, and rapid recovery in the event of disturbance.

Points to consider:

3.13.1 (S) The BFI shall conduct threat and vulnerability risk assessment (TVRA) to identify potential vulnerabilities and weaknesses of data centers in order to determine the necessary level and type of protection to ensure the security of data centers.

3.13.2 (S) To mitigate the single point of failure and ensure continuous operation, the BFI shall equip data centers with uninterruptible power supplies (UPS), backup generators, redundant cooling systems, and diversification of data communication and network paths.

3.13.3 (S) The BFI shall establish a secondary or disaster recovery data center, commensurate with business requirements, which shall be situated within a sufficient distance to ensure it remains unaffected when disaster occurs in the area of primary data center.

3.13.4 (S) Physical security and environmental controls for data centers shall be monitored 24/7. Escalation procedures and response plans for addressing incidents shall be established and periodically tested.

3.14 Virtualization and Containerization

3.14.0 Virtualization and containerization are technologies that enable efficient resource utilization and application deployment. Virtualization creates virtual machines, while containerization packages applications into portable units. Both technologies offer benefits like improved scalability, flexibility, and cost-effectiveness. However, they require robust security measures to protect against potential threats and vulnerabilities.

Points to Consider:

3.14.1 (S) The BFI shall establish and review a policy and procedures to manage virtual images and snapshots of virtualization and containerization.

3.14.2 (S) The virtualization and containerization procedures shall include, but not be limited to, security, creation, distribution, storage, usage, retirement and destruction of virtual images and snapshots to protect these assets.

3.14.3 (S) The BFI shall implement the following security controls on host virtual environment, which include, but are not limited to:

- Strong access controls for virtual environments, including operating systems, hypervisors, guest operating systems and any other related components;
- Enabling and monitoring logs for VMs and containers;
- Periodically scanning VMs and container images for vulnerabilities; and
- Using trusted images from reputable repositories for containers.

3.15 Internet of Things

3.15.0 The Internet of Things (IoT) refers to a network of interconnected physical devices that communicate and exchange data over the Internet. These devices can include smartphones, multifunction printers, security cameras, smart televisions, etc., which are embedded with sensors, software, and connectivity capabilities.

Points to consider:

3.15.1 (S) The BFI shall maintain all IoT devices in information asset inventory, detailing information such as their network connections and physical locations.

3.15.2 (S) The BFI shall assess and implement processes and strong access controls to mitigate risks arising from IoT devices.

3.15.3 (S) The BFI shall ensure that IoT devices are installed on a separate network segment from the network that provides access to the BFI's systems, and critical and sensitive data.

3.15.4 (S) The BFI shall ensure that IoT devices connecting to critical systems and confidential data are supported with secure algorithm for protecting data at rest, in transit, and in use from unauthorized access.

3.15.5 (S) The BFI shall procure IoT devices from trusted manufacturers and ensure that firmware is not hard coded so that security updates can be implemented.

3.16 Technology Refresh Management

3.16.0 Technology refresh management involves updating and replacing outdated systems, hardware, and software to keep BFIs' infrastructure efficient, secure, and aligned with business needs.

Points to consider:

3.16.1 (S) The BFI shall avoid using outdated and unsupported hardware or software, which could increase its risk exposure to security and stability.

3.16.2 (S) The BFI shall conduct a risk assessment for hardware and software approaching end-of-support (EOS) dates to evaluate the risks of continued use and implement effective risk mitigation measures.

3.16.3 (S) The BFI shall monitor the hardware's or software's EOS dates to avoid ceasing support and patch provision by service providers.

3.16.4 (S) The BFI shall establish a technology refresh plan for the replacement of hardware and software before they reach EOS dates.

3.16.5 (S) The continued use of outdated and unsupported hardware and software shall be approved by senior management. The approval shall be granted only for a period that reflects the identified risks and mitigation measures. The risk assessment shall be periodically conducted to ensure that the associated risks remain acceptable.

3.17 Supplier Relationships

3.17.0 Supplier relationships are referred to third party arrangements between BFIs and their suppliers, from which they purchase goods or services. These relationships are crucial for the efficient operation of BFIs' supply chain and can involve a wide range of activities, including negotiation, procurement, ongoing management, and performance evaluation. Examples of suppliers may include, but not be limited to, Internet service providers, application or managed service providers, business service providers or payment service providers.

Points to consider:

3.17.1 (S) The BFI shall establish and review a policy and procedures for managing supplier relationships related to IT goods and services from initiation to termination.

3.17.2 (S) The procedures for managing supplier relationships shall include, but not be limited to, the following:

- Supplier selection, onboarding, performance evaluation, contract management, issue resolution, and termination;
- Ongoing monitoring compliance to information security requirements based on criticality of the suppliers;
- Documentation of the types of suppliers (e.g., IT services, logistics, utilities, financial services, and IT infrastructure components), whom the BFI will allow to access its information;
- Incident and contingency processes associated with suppliers' access, outlining the responsibilities of both the BFI and suppliers; and
- Recovery and contingency arrangements to ensure the availability of services provided by the supplier.

3.17.3 (S) The BFI shall identify and implement information security controls to specifically address supplier risks. These controls shall be implemented by both the BFI and suppliers.

3.17.4 (S) The BFI shall conduct risk assessment to identify potential threats and vulnerabilities associated with suppliers based on their level of criticality. The results of assessment or re-assessment, including identified risks and proposed mitigation controls, shall be documented.

3.17.5 (S) Supplier agreements shall be established and documented to ensure that there is no misunderstanding between the BFI and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

3.17.6 The BFI shall document in the agreement the requirements for supplier including changes in services, contract termination, and unforeseen events. The following terms should be considered for inclusion in the agreement to satisfy the identified information security requirements, but not be limited to:

- Description of the information to be provided or accessed and methods of providing or accessing the information;
- Classification of information according to the BFI's classification scheme;
- Legal and regulatory requirements, including data protection, intellectual property rights, 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;
- List of supplier personnel authorized to access or receive the BFI's information;
- Procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the BFI's information by supplier personnel;
- Incident management requirements and procedures (especially notification and collaboration during incident remediation);
- Requirements 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.

Chapter 4 – Cybersecurity Management

4.0.0 BFIs should ensure the security of their IT environments by incorporating appropriate controls throughout their systems. It is imperative for BFIs to adhere to the following guidelines as integral components of the security policies to safeguard their IT environments against cyber risks.

4.1 Cyber Risk Management Framework

4.1.0 A cyber risk management framework (CRMF) is a structured approach designed to identify, assess, manage, and mitigate cyber risks within BFIs. It provides a systematic method to ensure that cybersecurity practices support business objectives and potential threats are effectively managed.

Points to consider:

4.1.1 (S) The BFI shall establish, review, and update cyber risk management framework (CRMF) periodically to manage cyber risks and enhance cyber resilience to deal with evolving cyber threat environment. CRMF shall be an integral part of the BFI's enterprise risk management framework.

4.1.2 (S) The framework shall set out risk appetites and tolerances for cyber risks and define processes and requirements to identify, assess, manage, monitor, and report on cyber risks.

4.1.3 (S) The BFI shall establish an enterprise risk management function who is responsible for implementing the CRMF at an enterprise-wide level.

4.1.4 (S) The BFI shall conduct regular cyber risk assessments including third-party risk as part of assessment to identify and evaluate potential cybersecurity threats and vulnerabilities to ensure a comprehensive understanding of their potential impacts on operation.

4.2 Cybersecurity Operation

4.2.0 Cybersecurity operation involves ongoing activities to mitigate BFIs from evolving cyber threats. A key component of this process is cyber event monitoring and detection, which enables proactive identification of threats, rapid incident response, and continuous improvement of security defenses. By investing in robust monitoring and detection technologies, BFIs can enhance their ability to protect BFIs' confidential information, maintain business continuity, and adapt to the evolving cybersecurity landscape.

Points to consider:

4.2.1 (S) The BFI shall establish a cyber incident playbook to guide its response to cyber incidents. The playbook shall include, but not be limited to, roles and responsibilities of incident response team (IRT) and standardized processes and procedures for incident detection, notification, containment, eradication, recovery, and post-incident analysis.

4.2.2 (S) The BFI may consider establishing a security operations center (SOC) or subscribing managed security services (MSS) to provide continuous monitoring, threat detection, and incident response capabilities.

4.2.3 (S) The BFI may consider deploying SOC, which operates on a 24/7 basis to provide continuous monitoring and threat detection.

4.2.4 (S) The BFI may consider equipping SOC with industry standard security information and event management (SIEM) tools that facilitate log consolidation, event correlation, incident management, forensic analysis, incident dashboard and report generation.

4.2.5 (S) The BFI shall subscribe to reputable threat intelligence services to proactively identify emerging cyber threats, uncover new cyber-attack techniques, and support the implementation of effective countermeasures.

4.2.6 (S) The BFI shall establish a procedure for investigating security incidents, which include, but not be limited to, forensics, evidence collection, preservation, log analysis, and interviewing.

4.2.7 (S) The BFI shall collaborate and share cyber threat information with the regulator.

4.3 Access Control

4.3.0 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 BFIs faces when access controls are not effective. To prevent unauthorized access, both logical and physical access controls need to be considered together.

Points to consider:

4.3.1 (S) The BFI shall establish and review an access control policy and procedures based on business and information security requirements.

4.3.2 (S) The access control procedure shall cover, but not be limited to, the following:

- Access right provisioning, de-provisioning and review;
- Proxy or ad hoc user access provisioning and de-provisioning;
- Deactivation of user IDs associated with critical applications when users are on long or prolonged leave;
- Modification of user access rights whenever there is a change in roles or responsibilities;
- Revocation of user access rights upon ending of employment contract;
- Prompt notification to information security function of any additions, deletions, or changes in user roles or profiles; and
- Access control matrix review.

4.3.3 (S) The BFI shall implement role-based access control (RBAC) and apply the principle of least privilege to ensure that individuals are granted only the minimum level of access necessary to fulfill their job responsibilities.

4.3.4 (S) The BFI shall establish an access control matrix that details roles or profiles and their associated permissions for critical or prone-to-cyberattack systems and applications. The access control matrix shall be periodically reviewed or updated when there are changes.

4.3.5 (S) The access rights granted to users shall be authorized and approved by asset owners.

4.3.6 (S) The BFI shall periodically conduct user access right review and user ID housekeeping for all active users to verify the user status and access privileges that are granted to users in systems and applications.

4.3.7 (S) For all critical systems and applications, the BFI shall maintain segregation between those initiating transaction and those responsible for verifying the transaction to ensure that no single employee/outsourced service provider could enter, authorize, and complete a transaction.

4.3.8 (S) The BFI shall establish a password policy and procedures to enforce strong password control for users' access to systems or applications.

4.3.9 (S) The password procedures shall cover, but not be limited to, the following:

- Minimum password length and history;
- Password complexity;
- Minimum and maximum password age;
- Change of password upon first login;

- Change of default user IDs and/or passwords for systems and applications;
- Account lockout threshold and duration;
- Management of inactive accounts; and
- Prohibition of sharing user IDs and passwords.

4.3.10 (S) System administrators, security officers, programmers, and staff with privileged access can cause significant damage to financial systems. Therefore, personnel with elevated or high privilege access shall be closely supervised, with all their activities logged, due to their inside knowledge and ability to bypass controls and security procedures. Some of the controls and security practices below may be considered:

- Implementing two-factor authentication for privileged users for all critical systems and applications;
- 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 logs of system activities performed by privileged users;
- Ensuring that privileged users do not have access to system logs, which their activities are being captured;
- Conducting regular audit or management review of the logs;
- Disabling or deleting any unnecessary ID with audit logs of deleted users retained;
- Prohibiting sharing of privileged IDs and their access codes; and
- Disallowing vendors and contractors from gaining privileged access to systems without close supervision and monitoring.

4.3.11 (S) The BFI may consider using automated solutions such as Privileged Access Management and Identity Access Management tools to enable effective access control and management of user IDs. Such solutions should also be managed effectively to ensure robust access management.

4.4 Remote Access

4.4.0 BFIs may sometimes provide employees, vendors, and others with access to the BFIs’ 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 BFIs’ systems or to support BFIs’ operations at remote locations. In some cases, remote access may be required by vendors to make emergency program fixes or to support a system. Remote access to the BFIs provides an attacker with the opportunity to manipulate and subvert BFIs’ systems from outside the physical security perimeter.

Points to consider:

4.4.1 (S) The BFI shall establish a remote access policy and procedures to ensure secure remote access.

4.4.2 (S) The remote access procedures shall cover the following, but not be limited to:

- Security control requirements;
- Remote access provisioning and de-provisioning including temporary and emergency remote access; and
- Monitoring and review of remote access.

4.4.3 (S) Remote access shall not be allowed unless a compelling business need exists and requiring management approval for remote access.

4.4.4 (S) The BFI shall periodically conduct review of remote access approval and withdrawal of those that no longer have a compelling business justification.

4.4.5 (S) The BFI shall periodically assess whether patches and updates for both anti-malware and host have been applied to remote access devices.

4.4.6 (S) The BFI shall use secure algorithm and network protocol to protect communication channels to restrict the risks related to network spoofing and data interception.

4.4.7 (S) The BFI shall implement a virtual private network (VPN) to secure communication data over the public network. Network segments shall be implemented to restrict remote access to authorized network areas, systems and applications within the BFI.

4.4.8 (S) All VPN connections shall be managed by a centralized VPN concentrator. Unauthorized direct VPN connections to other segments of the network shall not be allowed.

4.4.9 (S) The BFI shall maintain logs for remote access communications. These logs shall be included with the date, time, user, location, duration, and purpose for all remote access, documenting all activities conducted through remote access.

4.4.10 (S) The BFI shall ensure that all remote access sessions are automatically terminated after a defined period of inactivity.

4.4.11 (S) The BFI shall implement two-factor authentication for remote access (e.g., PIN based token card with a one-time random password generator, or token-based PKI).

4.4.12 (S) Remote access shall not be permitted through modems. If it is required, the following steps shall be taken, but not be limited to:

- Require an operator to leave the modems unplugged or disabled by default, to enable modems only for specific and authorized external requests;
- 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.

4.5 Cryptography

4.5.0 Cryptography provides confidentiality, integrity, authenticity, authentication, and nonrepudiation for data/information while it is in use, in transit and at rest. Digital signatures/certificates use cryptography as one of the key elements to provide authentication and authorization. Cryptographic keys are fundamental to encryption and decryption processes, underlying both digital signatures and certificates.

Points to consider:

4.5.1 (S) The BFI shall establish a cryptography policy and procedures to meet the information security policy's objectives.

4.5.2 (S) The BFI shall establish cryptography procedures aligned with industry standards and best practices. This procedure shall include, but not be limited to:

- Cryptographic controls, cryptographic techniques, and security requirements;
- Key management lifecycle including their generation, storage, usage, distribution, archiving, retrieval, revocation, and destruction; and
- Usage and management of cryptographic keys, digital signatures, and digital certificates

4.5.3 (S) The BFI shall conduct risk assessment to identify the required level of protection considering the type, strength, and quality of secure algorithm.

4.5.4 (S) The BFI shall use strong cryptographic algorithms and key lengths from national and/or international standards.

4.5.5 (S) The BFI shall ensure that all cryptographic keys are protected against modification, loss, unauthorized use, and disclosure.

4.5.6 (S) The BFI shall ensure that equipment, which is used to generate, store and archive keys, is physically protected and accessible only by authorized individuals.

4.5.7 (S) The BFI shall ensure that servers and applications used in production environments or for public-facing services have digital certificates signed by a trusted Certificate Authority (CA).

4.5.8 (S) The BFI may use key management system based on the business requirements following standards, 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 activation instructions;
- Securely storing keys and managing access controls;
- Implementing rules for changing or updating keys;
- Revoking and recovering of keys that are lost, corrupted, compromised, or no longer in used;
- Backing up or archiving keys for disaster recovery;
- Securely destroying keys at the end of their lifecycle; and
- Logging and auditing of key management related activities for accountability.

4.5.9 (S) Where signing documents or transactions in digital banking services involves the use of digital signatures, the BFI shall assess the suitability of using digital signatures and determine if there are relevant legal and regulatory requirements.

4.5.10 (S) The digitally signed documents or transactions shall be transmitted over a secure channel that allows the BFI to confirm the identity of customers e.g., the user account and e-mail address used to conduct the digitally signed documents or transactions are the same in the digital signature details.

4.5.11 (S) When using digital signatures for digital banking services, the BFI shall ensure that the digital signing process for making consent is clearly explained and comprehensible to customers, and agreed by both parties.

4.6 System Security

4.6.0 System security involves safeguarding hardware and software to prevent unauthorized access, malicious attacks, and cyberattacks.

Points to consider:

4.6.1 (S) The BFI shall establish and periodically review security baseline documents for hardware and software (e.g., operating systems, databases, network devices, applications, and endpoint devices) and applied uniformly on systems.

4.6.2 (S) The BFI shall conduct regular configuration review against security baseline documents to identify any implementation deviation from the documents.

4.6.3 (S) The BFI shall deploy anti-malware solutions to protect and detect malware infection. The anti-malware signatures shall be kept up to date with a regularly scanned for malicious files or anomalous activities.

4.6.4 (S) The BFI shall establish software and application whitelists to ensure what can be installed on BFI's endpoint devices. Any exception to the whitelist shall be reviewed by security function and approved by senior management.

4.6.5 (S) For endpoint devices those connect to the Internet, the BFI shall deploy endpoint detection and response (EDR) solutions to continuously monitor endpoint activities and scan for indicators of compromise.

4.6.6 (S) The BFI shall conduct a comprehensive risk assessment for bring your own device (BYOD) and implement necessary security measures to secure the use of personal devices in BFI's network.

4.7 Network Security

4.7.0 Network security safeguards computer networks from unauthorized access, misuse, and attack. Protecting the internal network required a combination of technology and process controls to ensure a secure network environment and resilience to cyber threats.

Points to consider:

4.7.1 (S) The BFI shall establish a network security policy and procedures to manage, monitor and maintain security of the computer network.

4.7.2 (S) The BFI shall establish network security procedures which include, but not be limited to:

- Roles and responsibilities of the network function and network security function;
- Types of network activities to be monitored;
- Logging and reporting mechanisms for unusual or suspicious activities; and
- Authorization for determining who is allowed to access specific networks and services.

4.7.3 (S) The BFI shall deploy network security devices, such as firewalls, anti-malware software, and intrusion detection and prevention systems, at critical junctures of its IT infrastructure to protect network perimeters.

4.7.4 (S) The BFI shall implement appropriate controls to ensure that all systems on the network are authenticated and all connections from untrusted systems are restrained. Network Access Control (NAC) solutions may be considered to implement in the network environment.

4.7.5 (S) Information services, information systems, and users shall be segregated into different network segments based on the systems' purposes, e.g., between a demilitarized zone (DMZ) and an internal network.

4.7.6 (S) The BFI shall ensure that the network services for its critical systems are highly reliable and designed with redundancy to avoid a single point of failure (SPOF) and protect against potential network faults and cyber threats.

4.7.7 (S) The BFI shall conduct network resilience assessment, including security design and network interconnections at least once every three years. The assessment shall be conducted by qualified expert either independent internal or external assessor.

4.8 Wireless Security

4.8.0 Wireless networks, which extend access to the corporate network, offer convenient connectivity for various devices across multiple locations, but they inherently pose greater security risks compared to wired networks. Unlike wired networks, wireless networks are susceptible to unauthorized monitoring and denial-of-service attacks, which can occur without a physical connection. Additionally, unauthorized wireless client devices could potentially connect to the corporate network through the wireless access point (WAP) to conduct man-in-the-middle attacks or interact with other wireless client devices.

Points to consider:

4.8.1 (S) The BFI shall establish and review a wireless security policy to secure their corporate network and prevent from unauthorized access through wireless networks.

4.8.2 (S) Wireless access to the BFI's corporate network shall be only provided on the basis of strong business cases and valid business purposes.

4.8.3 (S) The BFI shall ensure that the BFI's WAPs are manageable using enterprise management tools.

4.8.4 (S) The BFI shall ensure that the BFI's WAPs have their firmware periodically updated to protect against known vulnerabilities.

4.8.5 (S) The BFI shall ensure that the BFI's wireless service set identifier (SSID) is not publicly broadcasted, unless there are strong business cases and valid business purposes.

4.8.6 (S) The BFI shall ensure that each wireless client device connected to the BFI's corporate network fulfills the authorized configuration requirements and security baselines.

4.8.7 (S) The BFI shall ensure that all wireless networks are configured with the latest secure algorithm and authentication protocol.

4.8.8 (S) The BFI shall use wireless intrusion detection systems (WIDS) to identify and monitor rogue wireless devices and detect attack attempts and successful compromise.

4.8.9 (S) The BFI shall ensure that radio connection, such as NFC, Bluetooth, RFID, etc., is configured turned off by default or when not in use.

4.9 Data Security

4.9.0 Data security involves safeguarding all sensitive and critical information and data of BFIs from unauthorized access, tampering, or theft, whether digital or physical. To ensure effective protection, data should be classified according to classes or levels of sensitivity and criticality. A well-developed data classification schema enables BFIs to design and implement appropriate controls for each classification as an example provided in **Appendix 3.2**.

Points to consider:

4.9.1 (S) The BFI shall establish a data security policy and procedures to safeguard sensitive or critical data/information throughout the data lifecycle.

4.9.2 (S) The data security procedures shall cover, but not be limited to:

- Roles and responsibilities for data security function;
- Data/information classification based on levels of sensitivity and criticality;
- Secure data handling throughout data lifecycle (e.g., creation, storage, usage, transmission, and disposal of data); and
- Data security training and awareness for all staff.

4.9.3 (S) The BFI shall ensure that full disk encryption is implemented on endpoint devices and removable media that store confidential data/information.

4.9.4 (S) When disposing of systems and storage media, the BFI shall use secure methods such as physical destruction, purging or degaussing to ensure that data is unrecoverable. If there are contracts with third-party disposal firms, the BFI shall specify acceptable disposal methods and procedures with the firms.

4.9.5 (S) The BFI shall ensure that confidential data is encrypted using industry-standard methods both in transit and at rest.

4.9.6 (S) The BFI shall implement data security techniques, such as data masking, anonymization, pseudonymization, and tokenization, to safeguard confidential data by selecting or combining the techniques best suited to address specific data exposure risks and business requirements.

4.9.7 (S) The BFI shall establish and review a clear desk and screen guideline to ensure sensitive and critical information assets are not left unprotected, which could potentially lead to security breaches.

4.9.8 (S) The BFI shall restrict sensitive production data in non-production environments. In exceptional situations where such data needs to be used in non-production environments, approval shall be obtained from senior management. In addition, data security techniques shall be applied.

4.9.9 (S) The BFI may consider implementing mobile device management (MDM) solutions to secure, monitor, and manage data on mobile devices that connect to the BFI's network.

4.9.10 (S) The BFI may consider implementing appropriate technologies, such as data loss prevention (DLP) solutions, to prevent confidential data from being lost, accessed by unauthorized users, or leaked outside the organization's network perimeter. The state of data protection shall cover the following:

- **Data at rest:** This encompasses data stored in endpoint devices like laptops, desktops, portable storage devices, and mobile devices, as well as data in systems like servers, databases, backup media, and storage platforms;
- **Data in transit:** This refers to data traversing a network or being transported between sites; and
- **Data in use:** This refers to data being processed or actively used by a system.

4.10 Audit Trails

4.10.0 Audit trails maintain a record of user and system activities (e.g., operating systems, databases, network devices, applications, and endpoint devices). BFIs should ensure audit trails meet business, legal, and regulatory requirements, helping with audit, forensic investigation, and dispute resolution. They should cover key activities such as financial transaction, user account change, sensitive data access, system access, etc.

Points to consider:

4.10.1 (S) The BFI shall establish an audit trail policy and procedures to clearly define mandatory requirements for log management activities including generation, transmission, storage, analysis, and disposal.

4.10.2 (S) The audit trail procedures shall include, but not be limited to:

- Roles and responsibilities of individuals and teams who are involved in log management;
- Log sources and types of logs to be collected;
- Processes and tools used to manage and analyze logs for anomalies, trends, and potential incidents; and
- Methods for disposing of logs that are no longer required or have reached their retention period.

4.10.3 (S) The BFI shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

4.10.4 (S) The BFI shall enable audit logs of system activities performed by privileged users.

4.10.5 (S) The BFI shall ensure that a centralized network time protocol (NTP) server is used to synchronize time across all devices.

4.10.6 (S) The BFI shall ensure that log information is protected from unauthorized changes by using appropriate logging tools. This includes, but is not limited to, safeguarding against:

- Alteration 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.

4.10.7 (S) The BFI shall ensure event logs include, when relevant:

- User IDs;
- System activities;
- Dates, times, and details of events, e.g., log-on and log-off;
- Identities and locations of devices and/or systems;
- 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;
- File 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.

4.10.8 (S) The BFI shall integrate audit logs at least from critical systems into a centralized log server for real-time monitoring, correlation, and alerting.

4.10.9 (S) The BFI shall conduct periodic review of audit logs of privileged users to detect anomalies, suspicious activities, and security violations.

4.10.10 (S) Audit trails shall be secured and kept for as long as required by business requirements and regulations. The audit logs of user activities for critical systems shall be logged and maintained for at least three years for investigation and troubleshooting.

4.11 System Acquisition, Development and Maintenance

4.11.0 System acquisition, development, and maintenance encompass the lifecycle of a system, including assessing needs, acquiring or building, deploying, ongoing support, and maintenances. BFIs have different types of systems, such as core banking system, ATM, internet banking, mobile banking, enterprise resource planning (ERP) system, and customer relationship management (CRM) system.

Points to consider:

4.11.1 (S) The BFI shall establish a secure software development lifecycle (SDLC) policy and procedures to ensure that systems are acquired, developed, maintained, and disposed securely.

4.11.2 (S) The BFI shall establish secure SDLC procedures which encompass methodologies for each phase, including initiation/planning, requirement analysis, design, development, testing, deployment, maintenance, and decommissioning. Comprehensive documentation shall be produced corresponding to all phases.

4.11.3 (S) The BFI shall conduct vendor evaluation of acquired systems by taking into account of vendor sustainability and lock-in as require in chapter 7- **Technology Service Outsourcing**.

4.11.4 (S) The BFI shall enter into a source code escrow agreement to ensure the source codes for critical systems are accessible. If an escrow agreement cannot be implemented, the BFI shall identify an appropriate alternative.

4.11.5 (S) The BFI shall ensure that security requirements are considered during the early stages of system development or acquisition. At a minimum, these requirements shall include system access control, authentication, transaction authorization, data integrity, system activity logging, audit trails, security event tracking, and exception handling.

4.11.6 (S) Source code review shall be conducted for all critical applications. At a minimum, this shall be included after every major update, such as any software update released by the vendor categorized as major, any update requiring downtime for the applications, etc.

4.11.7 (S) The BFI shall ensure that the application source code is adequately protected and secured against unauthorized access.

4.11.8 (S) The BFI shall establish a methodology for rigorous system testing and ensure that adequate testing is performed before a system launch. The testing scope shall cover business logic, system functionality, security controls, and system performance.

4.11.9 (S) The BFI shall document, track, and address the issues identified during testing, including vulnerabilities, deficiencies, system defects or software bugs.

4.11.10 (S) The BFI shall ensure that the outcomes of all testing are documented in test reports with sign-off by the relevant stakeholders.

4.11.11 (S) The BFI shall periodically conduct system maintenance to ensure ongoing performance optimization, scalability, and reliability of systems during operation.

4.11.12 (S) The BFI shall define service level agreement (SLA) of systems and continuously evaluate the key performance indicators (KPIs) therein. Any breaches of the SLA shall be reported to senior management immediately.

4.11.13 (S) When decommissioning systems, the BFI shall minimize any disruption to customers and business operations and maintaining business service continuity.

4.12 Training and Awareness

4.12.0 Training equips employees with the skills necessary to perform their jobs more effectively and securely. Meanwhile, awareness programs foster a corporate culture that values security and negative consequences of security breaches. There is a vital need for an initial and ongoing technology training and information security awareness program.

Points to consider:

4.12.1 (S) The BFI shall establish a training and awareness policy that outlines the objectives, requirements, skills, behavior changes, and expected outcomes for employees, ensuring they are equipped with the necessary knowledge and skills in technology operation, information security, cybersecurity, and risk management.

4.12.2 (S) The BFI shall implement a training plan for IT personnel to obtain professional certifications based on skill gaps from recognized training providers. If deemed necessary, IT personnel shall acquire certifications such as information security, cybersecurity, project management, cloud operation, and other IT related domains.

4.12.3 (S) The BFI shall ensure the training for employees adequately covers the technology operation and provides sufficient knowledge for supporting business operation.

4.12.4 (S) The BFI shall establish information security training and awareness programs for board members, senior management, employees, and contractors, who are required to attend at least once a year.

4.12.5 (S) The BFI shall ensure information security training and awareness programs are repetitive and continuous for both new and existing employees. The program topics shall be updated periodically to reflect the current cyber threat landscape.

4.12.6 (S) The BFI shall ensure that information security training and awareness programs are conducted by experienced internal trainers or qualified external trainers from a reputable service provider.

4.12.7 (S) The following topics shall be incorporated as part of the information security training and awareness programs:

- 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;
- Relevant information security policies and procedures;
- Personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the BFI and external parties;
- Acceptable and appropriate usage of IT assets;
- Access controls including standards relating to passwords and other authentication requirements;
- Measures relating to proper email and internet usage;
- Physical protection;
- Remote access and use of mobile devices;
- Wi-Fi security best practices;
- Handling of confidential data/information;
- Social engineering; and
- Prompt reporting of any security incidents and concerns.

4.12.8 (S) The BFI shall provide information security training and awareness to customers, but not be limited to, the following:

- Social engineering;
- Education on securely conducting online transactions;
- Measures to mitigate technology risks;
- Secure PINs and security tokens; and
- Safeguarding mobile devices and any other devices used to access online banking services.

4.12.9 (S) The BFI shall incorporate a periodic testing and simulation exercise, such as phishing simulation, into the training program to assess and reinforce employees' ability to recognize and respond to security threats effectively.

4.12.10 (S) The BFI shall maintain record of educations, trainings, skills, experiences, and qualifications of employees.

4.12.11 (S) The BFI shall establish mechanisms for gathering feedback from participants on the training and awareness programs and for continually improving the training content and delivery methods.

4.13 Vulnerability Assessment and Penetration Testing

4.13.0 Vulnerability assessment (VA) and penetration testing (PT) are essential components of cybersecurity testing to enhance the security of BFIs' IT environment. Vulnerability Assessment involves a systematic evaluation of BFIs' IT environment to identify potential vulnerabilities and weaknesses of security controls. Penetration Testing goes beyond VA by simulating real-world cyberattacks to exploit vulnerabilities.

Points to consider:

4.13.1 (S) The BFI shall establish and review a policy and procedures for vulnerability assessment and penetration testing to enforce regular assessment and evaluate the security posture of the IT environment.

4.13.2 (S) The BFI shall establish procedures for VA and PT which outline, but are not limited to, roles and responsibilities of the team, types of assessments, frequencies of assessments and target resolution timeframes for remediation actions of identified vulnerabilities.

4.13.3 (S) The BFI shall deploy a combination of automated tools and manual techniques to regularly perform a comprehensive vulnerability assessment.

4.13.4 (S) The BFI shall ensure that vulnerability scanning is performed in an authenticated mode (e.g., configuring the scanner with administrator credentials) at regular intervals either with agents running locally on each endpoint device to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested.

4.13.5 (S) The BFI shall conduct penetration testing at least annually to conduct an in-depth evaluation of the security posture for critical systems by simulating actual attacks, using a combination of white-box, black-box, and gray-box testing.

4.13.6 (S) The BFI shall include, if possible, third-party systems and services in the scope of their VA and PT to ensure that external dependencies do not introduce security risks.

4.13.7 (S) The BFI shall ensure that vulnerabilities identified from VA and PT are remediated. Any unresolved vulnerabilities shall be tracked with clear accountability assigned.

4.13.8 (S) The BFI shall ensure the repeated vulnerabilities are addressed either by patching, implementing a compensating control, or documenting and accepting at a reasonable business risk. Such acceptance of business risks for existing vulnerabilities shall be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed resulting in increasing the risk.

4.13.9 (S) The information security function shall periodically provide status updates regarding the number of unmitigated, critical vulnerabilities, for each division/department, and the mitigation plan to senior management.

4.14 Adversarial Attack Simulation Exercise

4.14.0 Adversarial attack simulation exercises, also known as red team exercises, are crucial for BFIs to simulate real-world cyber threats and evaluate the efficiency of their security measures and the effectiveness of their incident response capabilities. This exercise aims to mimic actual cyberattacks, providing valuable insights into BFIs' ability to detect and respond to security incidents, thereby enabling continuous improvement in cybersecurity defenses.

Points to consider:

4.14.1 (S) The BFI shall conduct an adversarial attack simulation exercise at least every two years to assess and validate the effectiveness of its cybersecurity defense and response plan against cyber threats.

4.14.2 (S) The BFI shall define the objectives, scope, and scenario-based testing of the simulation exercises and ensure that activities are conducted under close supervision to minimize disruption to the BFI's business operations.

4.14.3 (S) All activities during the simulation exercises shall be monitored and logged for analysis and evaluation of response capabilities.

4.14.4 (S) The findings and recommendations with action plan from the simulation exercises shall be documented and reported to senior management and key stakeholders.

4.14.5 (S) The BFI shall incorporate the lessons learned from the simulation exercises into training programs, incident response plans, and the cyber incident playbook to enhance incident response capabilities.

Chapter 5 – Business Continuity Management

5.0.0 Business continuity management (BCM) is crucial for BFIs to oversee and enhance continuity, resilience, and proactive response capabilities. It provides a framework for BFIs to effectively anticipate, prepare, monitor, respond, and recover from disruption, such as incidents and natural disasters that can impact critical business functions and systems. This BCM also includes several underlying strategic plans such as business continuity strategy, business continuity plan (BCP), disaster recovery plan (DRP) and incident and emergency management plan (IEMP).

Points to consider:

5.0.1 (S) The BFI shall establish and review a business continuity management policy which includes, but is not limited to, organizational roles and responsibilities, processes, and resources to enhance resilience of the business operations and services.

5.0.2 (S) The BFI shall conduct a risk assessment to identify, analyze, and evaluate threats which may potentially disrupt the BFI's business operations and services. This analysis shall encompass threat scenarios but not limited to system outages, hardware malfunctions, human errors, security incidents, as well as complete failure of the primary data center.

5.0.3 (S) The BFI shall conduct a business impact analysis to identify and evaluate potential impact that interrupt to critical business operations and services as a result of disaster, incident, and emergency, including determination of MTD, recover time objective (RTO) and recovery point objectives (RPO).

5.0.4 (S) The BFI shall ensure that the data and system backup mechanisms meet the RTO and RPO requirements.

5.0.5 (S) The BFI shall develop business continuity strategies to achieve RTO and RPO, as required by relevant regulatory requirements for critical business functions and systems.

5.0.6 (S) The BFI shall establish a comprehensive business continuity plan (BCP) in relation to the BFI's nature, size, and complexity. The BCP shall include, but not be limited to, the following:

- Clear roles and responsibilities of the BFI's BCP execution team and relevant stakeholders;
- Documented plans, responses, and recovery procedures; and
- Escalation, notification, and communication procedures, including call trees and contact lists.

5.0.7 (S) The BFI shall establish a comprehensive disaster recovery plan (DRP) to respond to disasters and restore the affected IT critical systems back to a normal state within expected RTO and RPO.

5.0.8 (S) Incident and emergency management plan (IEMP) shall be developed to enable the BFI to respond to and recover from major events. It shall include, but not be limited to, roles and responsibilities, leadership, internal and external communication, and key personnel who represent all relevant business units to act during emergencies.

5.0.9 (S) Communication protocols for an emergency event shall include contact lists and communication channels to reach personnel and other stakeholders who may be called upon during an emergency. The contact list shall be distributed and accessible to key personnel and shall be verified and updated periodically.

5.0.10 (S) The BFI shall implement a business continuity training program to educate stakeholders on policies, objectives, business continuity plans, and personnel's roles and responsibilities.

5.0.11 (S) The BFI shall establish an exercise and testing program with clear objectives and detailed plans to validate the BFI's ability to restore critical business functions and critical systems. The program shall cover the IEMP, BCP and DRP.

5.0.12 (S) The exercise and testing program shall be conducted at appropriate time intervals and shall include various types of tests such as checklist, tabletop, simulation, parallel and full interruption.

5.0.13 (S) The BFI shall document and track all issues identified during the exercises and tests, including creating action plans with timelines for resolution. The exercise and test results shall be evaluated against objectives and success criteria, and any unresolved issues shall be documented with management approval.

5.0.14 (S) The BFI shall review the BCP, DRP and IEMP at least annually or when there are significant changes to business operations and the IT environment.

Chapter 6 – Digital Service Protection

6.0.0 Digital services include Internet banking, mobile banking, e-wallet, payment processing, self-service banking, and other banking activities that can be accessed and managed through digital platforms provisioned over the Internet. To safeguard data and maintain the security of digital services, BFIs adopt security control measures that are aligned with the associated risks with its respective type of services.

Points to consider:

6.0.1 (S) The BFI shall conduct risk assessment to identify and evaluate the relevant risks associated with digital services, both prior to and periodically thereafter launching the service. Proper risk management shall be performed to address relevant risks.

6.0.2 (S) The BFI shall conduct security assessments to identify vulnerabilities. The critical vulnerabilities shall be resolved prior to launching the digital services.

6.0.3 (S) The BFI shall set the limit on the number of failed logins or authentication attempts, and the period of inactivity for automatic logout.

6.0.4 (S) The BFI shall implement session management controls to prevent multiple concurrent logins by a single account.

6.0.5 (S) The BFI shall implement secure communication protocols and certificates pinning to prevent man-in-the-middle attacks.

6.0.6 (S) The BFI may consider implementing fraud detection solutions to monitor transactions for suspicious activities, such as unusual patterns or unauthorized access attempts, and take appropriate actions to mitigate risks.

6.0.7 (S) The BFI shall ensure that changes in customer’s mobile phone number or email address which is linked to digital services must be done through a secure mechanism with due diligence.

6.1 Internet Banking

6.1.0 Internet banking services can provide significant opportunities for BFIs. They may allow BFIs to expand their markets in traditional deposit-taking and credit extension activities, and to offer new products and services via the Internet.

Points to consider:

6.1.1 (S) The BFI shall implement at least two-factor authentication to validate customers' identities at each login session before allowing them to conduct any online transaction.

6.1.2 (S) The BFI shall ensure that secure authentication such as one-time password (OTP), used for authentication, has a limited validity period for each financial transaction. OTPs shall be generated using a secure, unpredictable algorithm and delivered to the user via a secure channel.

6.1.3 (S) The BFI shall implement web application firewall (WAF) to protect against Denial of Service (DoS) attacks, including rate limiting (limiting the number of requests that can be handled within a specific period), traffic filtering, and anomaly detection to identify and mitigate unusual patterns of activity that may indicate an attack.

6.1.4 (S) Internet banking web application shall not store sensitive information in HTML hidden fields, cookies, or any other client-side storage which may lead to compromise in the integrity of data.

6.1.5 (S) The BFI shall implement input validation, CAPTCHA, or random token to secure the Internet banking web application.

6.2 Mobile Banking

6.2.0 Mobile banking services allow customers to conduct transactions, check balances, transfer money, pay bills, and access other banking services through a mobile application. Mobile banking offers convenience, allowing banking services to be accessed anytime and anywhere using mobile devices.

Points to consider:

6.2.1 (S) The BFI shall implement at least two-factor authentication as a security measure for mobile application registration. This requires customers to provide both a password and additional authentication such as OTP sent via a secure channel to complete the registration process.

6.2.2 (S) The BFI shall implement a secure and reliable time-based one-time password (TOTP) mechanism. TOTP shall be generated using a secure, unpredictable algorithm and delivered to user via a secure channel.

6.2.3 (S) The BFI shall implement multi-factor authentication for high-value fund transfers whenever possible, requiring customers to provide the following authentication factors: something they know (e.g., password), something they have (e.g., OTP), or something they are (e.g., biometric data). Where possible, customers shall be able to set a limit on the per-transaction amount for payment and transfer.

6.2.4 (S) The BFI shall ensure the integrity and authenticity of the mobile application.

6.2.5 (S) The BFI shall implement code minification and code obfuscation techniques to prevent reverse engineering of the mobile application.

6.2.6 (S) The BFI shall implement security measures to detect and prevent installation of the mobile application on emulators and jailbroken or rooted devices.

6.2.7 (S) The BFI shall implement web application firewall (WAF) to protect against DoS attacks, including rate limiting (limiting the number of requests that can be handled within a specific time period), traffic filtering, and anomaly detection to identify and mitigate unusual patterns of activity that may indicate an attack.

6.2.8 (S) Mobile applications for customers shall be made available only through trusted mobile application repositories.

6.3 E-Wallets

6.3.0 E-wallets enable customers to conduct payment transactions by simply using phone number, and mobile payment application on mobile devices. They offer a convenient and secure way to make payment, whether online or in-store. If an e-wallet is web-based, BFI shall follow the **6.1 Internet Banking** of this guideline.

Points to consider:

6.3.1 (S) The BFI shall implement at least two-factor authentication as a security measure for E-wallet application registration. This requires customers to provide both a password and additional authentication via a secure channel to complete the registration process.

6.3.2 (S) The BFI shall establish limit on daily transaction and/or amount for each customer account, or as required by relevant regulations.

6.3.3 (S) The BFI shall implement multi-factor authentication for high-value fund transfers whenever possible, requiring users to provide the following authentication factors: something they know (e.g., password), something they have (e.g., OTP), or something they are (e.g., biometric data).

6.3.4 (S) The BFI shall implement code minification and code obfuscation techniques to prevent reverse engineering of the e-wallet application.

6.3.5 (S) The BFI shall implement security measures to detect and prevent installation of the application on emulators, and jailbroken or rooted devices.

6.3.6 (S) E-wallet applications for customers shall be made available only through trusted application repositories.

6.4 Self-Service Terminals

6.4.0 Self-service Terminals (SST) are devices for customers to conduct transactions by themselves such as withdrawing and depositing cash, paying bills, transferring funds, etc. SSTs include devices such as Automated Teller Machine (ATM), Cash Deposit Machine (CDM), Cash Recycler Machine (CRM), Smart Teller Machine (STM) and kiosks.

Points to consider:

6.4.1 (S) The BFI shall install anti-skimming solutions on SST devices to detect and prevent the presence of unauthorized devices placed over or near card entry slots.

6.4.2 (S) The BFI shall install an alarm system with a triggering mechanism which alerts to appropriate staff for any unauthorized opening or tampering of the physical components of SSTs. Follow-up responses and corrective actions shall be taken on a timely manner.

6.4.3 (S) The BFI shall ensure that SST devices equip with a PIN pad shield to prevent shoulder surfing and protect customer’s PIN.

6.4.4 (S) The BFI shall implement tamper-resistant keypads or secure PIN entry devices to ensure that customer’s PIN is entered securely and encrypted during transmission to prevent interception by unauthorized parties.

6.4.5 (S) The BFI shall install closed-circuit cameras and video surveillance cameras with adequate lighting to ensure high quality of CCTV footage and clear video images of customer conducting transaction.

6.4.6 (S) The BFI shall deploy an anti-malware solution for SSTs to detect and protect against malware infection. The anti-malware signatures shall be kept up to date. A regular scan shall be conducted to detect malicious files or anomalous activities.

6.4.7 (S) The BFI shall ensure that SSTs’ operating system is running on a secure version that receives ongoing support from vendors for security patches to address any vulnerability.

6.4.8 (S) The BFI shall monitor SSTs to detect downtime and ensure timely intervention to minimize service disruption.

6.4.9 (S) The BFI shall periodically conduct physical assessment, both before and after installation, of all SSTs’ locations, including those at third-party sites, to ensure that adequate security measures are in place.

6.5 Payment Cards

6.5.0 Payment cards allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payment at the merchant, or not presenting when they purchase items over the Internet. Payment cards also provide cardholders with the convenience for withdrawing cash at any ATM machine or transacting through merchants.

Points to consider:

6.5.1 (S) The BFI shall use the Payment Card Industry Data Security Standard (PCI DSS) for international payment card schemes or use equivalent domestic payment card security requirements for proprietary card management for compliance assessment.

6.5.2 (S) The BFI shall ensure full compliance with payment card security requirements. An implementation plan shall be developed for any non-compliant points with specific actions and timelines to address them.

6.5.3 (S) The BFI shall implement the EMV standard for payment cards.

6.5.4 (S) The BFI shall implement secure authentication methods for card-not-present transactions conducted via the Internet to reduce the fraud risk.

6.5.5 (S) The BFI shall promptly notify cardholders through transaction alerts whenever transaction is made on their payment cards. These alerts include details about the transaction, but are not limited to, source, amount, date, and time.

6.5.6 (S) The BFI shall implement robust fraud detection systems to identify, detect and prevent fraudulent activities. These methods and capabilities may be considered including behavioral scoring, correlation, etc.

6.5.7 (S) The BFI shall set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

6.5.8 (S) The BFI shall monitor and investigate transactions that significantly deviate from a cardholder's usual usage patterns and shall obtain the cardholder's authorization before completing these transactions.

6.6 SWIFT

6.6.0 SWIFT stands for the Society for Worldwide Interbank Financial Telecommunication, is a cooperative organization that operates a secure messaging network for member financial institutions worldwide to send and receive information regarding financial transactions.

Points to consider

6.6.1 (S) The BFI shall use the latest SWIFT Customer Security Controls Framework (CSCF) to perform their compliance assessment based on the architecture used by the BFI.

6.6.2 (S) The BFI shall ensure full compliance with all mandatory requirements of the SWIFT CSCF. An implementation plan shall be developed for any non-compliant points with specific actions and timelines to address them.

6.6.3 (S) SWIFT CSCF assessor shall rotate at least once every three years.

Chapter 7 – Technology Service Outsourcing

7.0.0 Technology service outsourcing is 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, including agreements for a limited period, that would normally be undertaken by BFIs themselves. Common areas where BFIs have outsourced functions include technology infrastructure and operations (e.g., teleworking, call centers, payment card services, payment gateways, and customer verification).

Points to consider:

7.0.1 (S) The BFI shall establish and review a technology service outsourcing policy and procedures that cover the entire lifecycle of outsourcing relationship.

7.0.2 (S) Technology service outsourcing procedures shall include, but not be limited to, the following: defining service requirements and strategic goals, developing request for proposal, evaluating proposal, selecting vendor, negotiating contract terms, monitoring outsourced arrangement, and establishing termination and exit strategies.

7.0.3 (S) The BFI shall ensure that technology service outsourcing arrangements are approved by the Board.

7.0.4 (S) The BFI shall perform a risk assessment to identify, evaluate, and mitigate the relevant risks associated with technology service outsourcing arrangements.

7.0.5 (S) The BFI shall conduct due diligence on third-party service providers before engaging or renewing an outsourcing arrangement. The due diligence shall be documented as part of the monitoring and control procedures within outsourcing arrangement. The due diligence shall include, but not be limited to, evaluation of experience, reputation, financial sustainability, and ability to comply with applicable laws and regulations.

7.0.6 (S) When engaging an outsourcing arrangement with third-party service providers outside Cambodia, the BFI shall consider, but not be limited to, the following as part of their due diligence, and on a continuous basis:

- Political, social, and economic conditions;
- Legal and regulatory environments in the foreign country; and
- The ability to monitor the third-party service providers and execute its business continuity management and exit strategy.

7.0.7 (S) The BFI shall maintain caution lists and scoring for service providers. Where appropriate, the BFI may seek independent review and market feedback to complement internal assessment.

7.0.8 (S) The BFI shall have a non-disclosure agreement (NDA) signed with third-party service providers when confidential data and information are shared to ensure that they are fully aware of the legal consequences of disclosure of confidential data and information.

7.0.9 (S) When using multiple service providers collaborating to deliver an end-to-end solution, the BFI shall either designate one service provider as the 'Lead Service Provider' to manage other service providers or independently enter stand-alone contracts with each service provider.

7.0.10 (S) The BFI shall ensure that outsourcing arrangements are governed by legally enforceable written contracts. Contract terms shall be clear and understandable to both the BFI and service providers.

7.0.11 (S) The BFI shall ensure that the storage of its data is at least logically segregated from the other clients of the third-party service provider. In the event of termination of outsourcing agreement, the BFI shall ensure that all confidential data is retrieved and destroyed from the service provider.

7.0.12 (S) The BFI shall ensure that any critical system hosted by third party service providers has strong recovery and resumption capabilities in the event of failure or unsatisfactory performance.

7.0.13 (S) The BFI shall report to the regulator, where the scale and nature of functions outsourced are significant, or when data pertaining to Cambodian operations are in use, at rest and in transit outside Cambodia.

7.0.14 (S) When there is outsourcing arrangement with parent banks, subsidiaries, foreign head office, etc. The BFI shall ensure the respective responsibilities are clearly defined and documented in outsourcing agreement.

7.0.15 (S) The BFI shall ensure its third-party service providers comply with all relevant regulatory requirements prescribed in this guideline.

7.0.16 (S) The BFI shall ensure that third-party service providers comply with BFI's information security policy and procedure.

7.0.17 (S) For outsourcing arrangements of critical technology services, the BFI shall include provisions in the contract that:

- Allow the BFI to conduct outsourcing audits of third-party service providers or to obtain internal control-related reports from internal or external audits; and
- Allow regulators to have access and inspection rights over third-party service providers, and subcontractors, and to obtain relevant documents of the contracted service and internal control-related reports from internal or external audit.

7.0.18 (S) The BFI shall ensure that independent audits of the scope of outsourcing audit include, but are not limited to, assessing security controls of service providers and subcontractors, incident response processes, and compliance with outsourcing contracts.

7.0.19 (S) The BFI shall establish service level agreements to clearly define performance expectation, business continuity and penalty for failure to meet the agreed-upon requirements.

7.0.20 (S) The BFI shall include a clause in the outsourcing contract that allows for the termination of the outsourcing agreement in the event the third-party service provider fails to meet their obligations or under other force majeure conditions such as:

- The service provider changes ownership;
- The service provider goes out of business;
- There is a security breach or loss of confidential information; or
- The service provider fails to meet the agreed service level agreement.

Chapter 8 – Enabling Technologies

8.0.0 Cambodia's rapid FinTech advancements are outpacing traditional regulatory frameworks. To ensure responsible innovation and data protection, BFIs should adopt standards and best practices when implementing emerging technologies, even in the absence of specific local regulations. While FinTech innovation is driven by a range of enabling technologies, including cloud computing, application programming interfaces, big data analytics, artificial intelligence and machine learning, distributed ledger technology and blockchain technology, tokenization, biometrics, chatbot and social media. These technologies are transforming the financial landscape by increasing efficiency, improving customer experiences, and driving innovation.

Points to consider:

8.0.1 (S) When implementing enabling technologies, the BFI shall establish policies and procedures for each respective enabling technology that cover governance, security, and use. The policies shall be periodically reviewed and updated.

8.0.2 (S) Before implementation of new enabling technologies, the BFI shall conduct a comprehensive study with risk assessment and report to NBC.

8.0.3 (S) The BFI shall ensure that the implementation of new enabling technologies is supported by sufficient resources with the necessary skills, knowledge, and expertise.

8.0.4 (S) The BFI shall consider using relevant standards to guide implementation and risk management for new enabling technologies where applicable.

8.1 Cloud Computing

8.1.0 Cloud computing, also referred as cloud, is the delivery of computing services, including storage, processing power, network, and applications over the Internet. These services are hosted and managed by cloud service providers (CSP), allowing users to access and use them remotely without the need to own or maintain physical infrastructure. Examples of cloud services include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Security concerns in cloud services primarily involve data protection, privacy, compliance, and unauthorized access.

Points to consider:

8.1.1 (S) The BFI shall establish a cloud risk management framework or integrate it with the existing Technology Risk Management Framework and Cyber Risk Management Framework to manage the risk associated with cloud adoption.

8.1.2 (S) Before implementing cloud, the BFI shall conduct a comprehensive study on the risk associated with specific geographic locations of the data hosted in the cloud and seek prior approval from NBC.

8.1.3 (S) The BFI shall conduct comprehensive due diligence of CSPs before engaging with them. The due diligence shall include, but is not limited to, background, experience, reputation, financial sustainability, certifications (e.g., ISO27001), service organization control (SOC) reports, and ability to comply with applicable laws and regulations.

8.1.4 (S) When selecting a cloud service provider, the BFI shall consider interoperability, portability, and vendor diversity measures before entering into any agreement to prevent vendor lock-in and vendor concentration risk.

8.1.5 (S) The BFI shall ensure a proper shared responsibility model is formulated between a cloud service provider and the BFI, which indicates CSP's responsibilities for "Security-of-the-Cloud" and the BFI's responsibilities for "Security-in-the-Cloud”.

8.1.6 (S) The contract between the BFI and the cloud service provider shall include, but not be limited to:

- The name of the cloud service provider and full contact information;
- Clear responsibilities for both parties;
- Geographic locations of data storage and processing, trans-border data flows, business continuity, log retention, data retention, and audit trails;
- Specific activities for incident response;
- Ownership of intellectual property, unilateral contract termination, liability, obligation, and exit clause;
- Notification or approval requirements for the use of sub-contractors (e.g., fourth parties); and
- Penalty clause for failing to adhere to the service level agreement.

8.1.7 (S) The BFI shall develop a comprehensive cloud exit strategy before implementing cloud services. This strategy shall include identifying alternative cloud service providers or considering move back to on-premise infrastructure to address potential business disruption.

8.1.8 (S) The BFI shall ensure that cloud service providers protect the intellectual property, trade secret, and confidential customer information hosted on their cloud platforms.

8.1.9 (S) The BFI shall maintain an asset inventory of all systems hosted on cloud services with clear ownership.

8.1.10 (S) The BFI shall implement multi-factor authentication for users with privileges to configure cloud services.

8.1.11 (S) The BFI shall conduct regular security assessments on cloud workloads to evaluate the security posture. The scope shall include, but not be limited to, evaluation of security configurations, settings, and access control management.

8.1.12 (S) The BFI shall assess and monitor the cloud service provider's security controls to safeguard systems and data in the cloud as part of an enterprise-wide IT security monitoring service. The activities shall include requesting, receiving, and reviewing security and activity reports from the cloud service provider (e.g., SOC reports, independent audit reports, and ISO certification reports) to ensure that the controls are implemented and operated effectively.

8.1.13 (S) Where applicable, a hardware security module (HSM) is used for generating, storing, and managing the keys and is hosted in a higher control environment (e.g., own on-premise IT infrastructure) rather than with the CSP.

8.1.14 (S) For applications requiring high availability, the BFI shall ensure that CSP has appropriate cloud redundancy or fault-tolerant capability (e.g., use of the auto-scaling feature to enable auto-recovery of failed services) and other appropriate features are enabled for the cloud workloads.

8.1.15 (S) To prevent service disruption, the BFI shall ensure that cloud workloads are deployed in multiple geographically separated data centers (e.g., "zones" or "regions") to mitigate location-specific issues.

8.1.16 (S) The BFI shall proactively monitor the maintenance schedule, service disruption, change to services, and end-of-life of services, announced by CSPs via their websites or other official means.

8.2 Application Programming Interface

8.2.0 Application Programming Interface (API) allows different applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIs that provide developers with programmatic access to a software application or web service. BFIs may collaborate with third parties to develop open APIs for providing products and services to customers or other stakeholders. Therefore, it is important for BFIs to establish adequate safeguards to manage the development and provisioning of APIs for secure delivery of products and services.

Points to consider:

8.2.1 (S) The BFI shall implement security controls and ensure adequate system capacity to handle high volumes of API call requests to mitigate cyber threats, such as DoS attacks within the API gateway.

8.2.2 (S) The BFI shall periodically conduct security assessment of APIs to identify and address potential security weaknesses.

8.2.3 (S) The BFI shall implement strong security measures, including authentication and authorization, to protect sensitive data via APIs. API keys shall be protected using secure cryptographic algorithms and protocols. API access tokens shall have expiration times set to prevent their reuse.

8.2.4 (S) The BFI shall implement detective measures, including real-time monitoring and alerting technologies, to track API usage, monitor performance, and detect suspicious activities.

8.2.5 (S) The BFI shall establish a process for promptly revoking API keys or access tokens in the event of a security breach.

8.2.6 (S) When the BFI offers an API to the public, it shall be made available only through the BFI's official website and/or authorized third-party official website with clear terms of use and comprehensive documentation for developers.

8.2.7 (S) The BFI shall ensure the following measures for the API usage, which include, but not be limited to:

- Restrict responses to codes or instructions only, when possible;
- Clear data when a session is terminated or idle after a certain period; and
- Store data temporarily on the API for the response data on a need basis only.

8.2.8 (S) The BFI shall manage and monitor who has requested to use and/or who has subscribed to integrate the API into other systems by requiring third parties to register before accessing the API services.

8.2.9 (S) The BFI shall implement an API version control that includes, but is not limited to, major and minor releases, backward compatibility, minimum support period, disabling of obsolete versions, and communication (e.g., official website) of any update to third parties.

8.3 Big Data Analytics

8.3.0 Big data refers to large and complex datasets, which include structured and unstructured data, generated across various systems, processes, and data sources. Big data analytics can uncover valuable insights to enhance data-driven decision making, business operation, risk management, forecasting, customer experience, and innovation.

Points to consider:

8.3.1 (S) The BFI shall establish and review a data governance framework to ensure the accuracy, reliability, and governance of data to ensure adequate control throughout the data governance lifecycle (e.g., generation, collection, processing, storage, management analysis, virtualization, and interpretation).

8.3.2 (S) The BFI shall ensure data privacy, fairness, and ethical considerations in big data analytics processes.

8.3.3 (S) The BFI shall implement data quality management processes to continuously monitor and improve data quality throughout the lifecycle to maintain acceptable quality and fit for purposes.

8.3.4 (S) The BFI may consider implementing comprehensive data lineage process for data elements to track the flow of data from the source, movement, transformation and end-use.

8.3.5 (S) The BFI shall periodically review and validate the data and models used for big data analytics decisions to prevent the use of biased data or algorithms.

8.3.6 (S) The BFI shall verify the results of decisions based solely on big data analytics in cases where the decisions significantly affect customers, and ensure that customers are given the opportunity and sufficient support to challenge or respond to such decisions.

8.3.7 (S) The BFI shall remain accountable for the outcomes and decisions resulting from the use of big data analytics.

8.4 Artificial Intelligence and Machine Learning

8.4.0 Artificial intelligence and machine learning (AI/ML) are interconnected fields of computer science designed to create advanced systems that can simulate human cognitive functions and learn from data. While AI encompasses a broad range of technologies aiming at mimicking human intelligence, ML is a subset focusing on developing algorithms that improve through experience. In banking, AI/ML hold substantial potential for enhancing customer experience and operational efficiency. However, their adoption involves significant risks that must be managed through robust frameworks.

Points to consider:

8.4.1 (S) The BFI shall periodically assess AI/ML systems for compliance with internal policies and relevant laws and regulations.

8.4.2 (S) The BFI shall conduct a comprehensive risk assessment to evaluate and monitor the risks associated with the use of AI/ML and seek prior approval from the NBC.

8.4.3 (S) The BFI shall ensure that privacy by design and security by design based on standards are implemented for AI/ML systems.

8.4.4 (S) The BFI shall periodically review and validate the data and models used for AI/ML-driven decisions to prevent the use of biased data or algorithms.

8.4.5 (S) The BFI shall ensure that AI/ML systems are used in an ethical way, such as respect for human autonomy, prevention of harm, fairness, non-discrimination, transparency and explainability.

8.4.6 (S) The BFI shall ensure technical robustness and safety of AI/ML systems, including resilience to attack, fall back plan, accuracy, reliability, and reproducibility.

8.5 Distributed Ledger Technology and Blockchain Technology

8.5.0 Distributed ledger technology (DLT) refers to technology used for recording and sharing data across multiple ledgers. This technology allows for transaction and data to be recorded, shared, and synchronized across a distributed network of different network participants. Blockchain technology (BT) is a subset of distributed ledger technology. Blockchain employs cryptographic algorithm to record and synchronize data across a network in decentralized, immutable, and secure manner.

Points to consider:

8.5.1 (S) The BFI shall establish, and review secure key management procedures, including key generation, storage, access control, and recovery process.

8.5.2 (S) The BFI shall implement robust security measures to safeguard DLT/BT systems against unauthorized access and cyber threats.

8.5.3 (S) The BFI shall implement a secure identity and access management, including the processes and technologies used by BFI to authenticate and authorize an individual to access DLT/BT systems.

8.5.4 (S) The BFI shall implement fraud prevention measures to address issues arising from transactions recorded on DLT/BT systems.

8.5.5 (S) When implementing smart contracts, the BFI shall conduct and evaluate a security assessment and auditability to ensure they function as intended and does not contain vulnerabilities.

8.5.6 (S) The BFI shall periodically perform security assessment and audit of DLT/BT systems to identify and remediate potential vulnerabilities.

8.5.7 (S) The BFI shall implement private/permissioned DLT/BT systems that restrict participants or nodes to only authorized entities within the designated network.

8.5.8 (S) The BFI shall implement secure consensus algorithm for DLT/BT platform by taking into account level of decentralization, scalability, and security.

8.6 Tokenization

8.6.0 Tokenization is the process of replacing actual data such as financial account information, credit card information, or personally identifiable information with an alternate code called a “token”. The token is a reference that maps back to the data through a tokenization system. This method enables BFIs to safeguard data while still allowing its use for business purposes and minimizing risk exposure.

Points to consider

8.6.1 (S) The BFI shall establish and review secure token management procedures, which include, but are not limited to, generation, storage, usage, and access control.

8.6.2 (S) The BFI shall ensure the tokenization system is designed to be resilient and secure against reverse-engineering or tracing tokens back to the original data.

8.6.3 (S) The BFI shall ensure that tokenization system is implemented in accordance with industry standards and information security requirements.

8.6.4 (S) The BFI shall periodically perform security assessments and audits of tokenization systems to identify and remediate potential vulnerabilities.

8.6.5 (S) The BFI shall ensure that the token vault, which stores the mapping between tokens and data, is protected with secure encryption and access controls.

8.6.6 (S) The BFI shall ensure that the tokenization system, including the token vault, maintains logging of all activities, such as token generation, mapping, access, and deactivation.

8.6.7 (S) The BFI shall establish a process for token requests where authorized systems initiate requests for tokenization of data, using secure communication methods and identity validation of the requesting system.

8.6.8 (S) The BFI shall ensure that the token service provider, which is a third-party providing tokenization services to the BFI, implements a tokenization system which is reputable and compliant with relevant industry standards, and has access to only the token and not the original data.

8.7 Biometrics

8.7.0 Biometrics refer to automated recognition of individuals based on their biological and behavioral characteristics. It covers a variety of technologies, in which unique identifiable attributes of people are used for identification and authentication. Biometrics are used as an alternative method of identification and authentication to gain access to BFIs' digital services.

Points to consider

8.7.1 (S) The BFI shall obtain consent from individuals to use their biometric data for the purposes of identification and authentication for authorized services.

8.7.2 (S) Where biometric technologies are used for identification and authentication, the BFI shall ensure that biometric data is encrypted both at rest and in transit.

8.7.3 (S) The BFI shall calibrate the biometric system to ensure the false acceptance rate (FAR), and false rejection rate (FRR) are balanced to an acceptable level, minimizing both unauthorized access and false rejection.

8.7.4 (S) In the event that biometric technology is unavailable or nonfunctional, the BFI shall offer an alternative secure method for authentication.

8.7.5 (S) The BFI shall ensure that biometric data is stored in a secure environment, with strict access controls to prevent unauthorized personnel from accessing, modifying, or processing the data for purposes other than consented.

8.7.6 (S) The BFI may consider conducting a conformance testing using reliable software solutions to ensure that biometric systems meet the specified requirements.

8.7.7 (S) The BFI shall ensure that biometric data is securely sanitized once it is no longer used.

8.8 Chatbot

8.8.0 Chatbots are used in various contexts, such as customer support, virtual assistance, and website live chat to automate communication and provide quick, efficient responses to user queries. They interact with users via text or voice, responding to questions and performing tasks based on predefined rules or learned patterns.

Points to consider

8.8.1 (S) The BFI shall ensure that the information provided by the chatbot is accurate, relevant, and transparent to the customer's query.

8.8.2 (S) The BFI shall inform customers when they are interacting with a chatbot, not a human.

8.8.3 (S) The BFI shall ensure that customers' consent for data collection and processing is obtained explicitly at the beginning of the chatbot interaction.

8.8.4 (S) The BFI shall provide options for customers to escalate issues or seek further assistance if the chatbot is unable to resolve their query or if the customer prefers to interact with staff.

8.8.5 (S) The BFI shall collect customer feedback on the chatbot's performance and experience to continuously improve its accuracy, relevance, and customer satisfaction.

8.8.6 (S) The BFI shall periodically conduct a review and testing on the chatbot to ensure the information or query requested by customers is accurate, relevant, and transparent.

8.9 Social Media

8.9.0 Social media offers BFIs a strategic opportunity to engage with customers, strengthen brand recognition, and support business growth through targeted outreach, customer interaction, and enhanced visibility in the digital space. Since social media platforms are operated by third-party providers, BFIs should carefully assess the associated risks and determine which platforms are most suitable for their need.

Points to consider

8.9.1 (S) The BFI shall ensure that the social media account is a business account and verified, if possible, on the chosen social media platform.

8.9.2 (S) The BFI shall ensure that the content of the social media is managed by the content administrator and the social media account is limited to the authorized personnel only.

8.9.3 (S) The BFI shall enable secure authentication methods to enhance security and prevent unauthorized access.

8.9.4 (S) The BFI shall ensure that the social media account used for business purposes is not used for personal purposes or linked to unrelated services.

8.9.5 (S) The BFI shall monitor and control the social media contents, the profiles followed, friends added, pages liked, or groups joined. Where possible, the BFI shall review their account's followers or friends.

8.9.6 (S) Comment features shall be disabled unless administered by the content administrator. Comments that are potentially harmful or illegal shall be removed.

8.9.7 (S) The BFI may consider implementing brand protection to monitor, manage, and safeguard reputation across multiple platforms from cyber threat actors such as typo-squatting, defacements, rogue apps, and brand impersonation in social media.

8.10 Near Field Communication

8.10.0 Near field communication (NFC) is a short-range communication technology that enables two devices to exchange data when brought within a few centimeters of each other. NFC chips can be embedded in a device (e.g., payment cards, smart phones, smartwatches, or other NFC-enabled devices) to enable it to act as a contactless payment card.

Points to consider

8.10.1 (S) The BFI shall ensure that merchants use only approved reader devices provided by the BFI. If merchants use NFC-enabled devices from third-party providers, the BFI shall ensure that those devices comply with the BFI's internal security requirements.

8.10.2 (S) The BFI shall ensure that NFC implementation complies with relevant standards, laws, and regulations.

8.10.3 (S) The BFI shall ensure that NFC is disabled when not in use to prevent unauthorized transactions and accidental interaction with compromised NFC tags.

8.10.4 (S) The BFI shall enable secure authentication methods via payment applications or systems for high value transactions and on NFC registration.

8.10.5 (S) The BFI shall implement end-to-end encryption for NFC-enabled payment to protect transaction data.

8.10.6 (S) The BFI shall ensure that the software of NFC-enabled devices is regularly updated to address security vulnerabilities.

8.10.7 (S) The BFI shall ensure that all payments made using the NFC feature are recorded in the applications or systems as usage or transaction history, regardless of the transaction value.

Chapter 9 – Customer Personal Data Protection

9.0.0 When offering products and services to customers, it is vital for BFIs to protect customers' interests to foster trust. Customer personal data plays a key role in business operations, offering significant opportunities for BFIs to innovate and improve their services. However, it is equally important for BFIs to comply with relevant laws and regulations.

Points to consider

9.0.1 (S) The BFI shall establish and review customer personal data protection or privacy procedures to include, but not be limited to:

- Roles and responsibilities of the function for protecting customer personal data;
- Types of customer personal data collected and levels of protection;
- Processes to enable individuals to exercise their rights; and
- Processes to notify the affected individuals and relevant regulators in compliance with applicable laws and regulations.

9.0.2 (S) The BFI shall clearly indicate the purpose of data collection and obtain consent from customers before collecting their data. This consent shall be freely given, well-informed, specific, and unambiguous.

9.0.3 (S) The BFI shall ensure customer personal data collected maintains its accuracy, consistency, integrity, uniqueness, completeness and currentness.

9.0.4 (S) The BFI shall establish relevant processes for customers to access, rectify, delete, restrict, and transfer their personal data.

9.0.5 (S) The BFI shall retain customer personal data only as long as necessary for its purpose, as required by laws, or upon request for deletion from customers.

9.0.6 (S) Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA) shall be conducted and reviewed upon critical incidents related to customer data or at least every 3 years.

9.0.7 (S) The BFI shall implement privacy by design principles, ensuring that customer personal data protection measures are integrated into the development of systems, products, or services.

9.0.8 (S) The BFI shall implement data minimization principles, collecting only the customer's personal data that is necessary for specific purposes.

9.0.9 (S) The BFI shall establish a data protection function responsible for overseeing customer personal data protection in the BFI and compliance with relevant laws and regulations.

9.0.10 (S) The BFI shall ensure that all third-party service providers processing customer personal data on its behalf comply with the BFI's customer personal data protection or privacy policy as well as relevant laws and regulations.

9.0.11 (S) Customer personal data protection or privacy policy shall be incorporated into the BFI training and awareness program to ensure that relevant staff comprehensively understand their roles and responsibilities in safeguarding the data.

9.0.12 (S) The BFI shall periodically conduct audits on customer personal data protection to identify and mitigate risks associated with customer personal data.

Chapter 10 – Information Technology Audit

10.0.0 With the increasing adoption of technology by BFIs, the complexities within the information technology (IT) environment have given rise to considerable technology-related risks, requiring effective management. This led BFIs to strengthen their internal control framework, using various standards and control requirements. As a result, BFIs' management need assurance on the effectiveness of the implemented internal controls, and expects the IT 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. Hence, there is a need for BFIs to re-assess the IT audit processes, and ensure that IT audit objectives are effectively met.

Points to consider:

10.0.1 (S) The BFI shall establish the IT audit function to assess independently and objectively the controls, reliability, and integrity of the BFI's IT environment.

10.0.2 (S) The BFI shall define roles and responsibilities, objectives, delegation of authority of IT audit function, audit management, and the audit committee as part of audit charter or policy. The charter or policy shall be approved by the audit committee and the board.

10.0.3 (S) The BFI shall ensure that the auditor's independence is maintained throughout the audit engagement. This independence shall be documented as part of an annual declaration to the audit committee and the board, which outlines any potential conflicts of interest and the measures taken to mitigate them.

10.0.4 (S) The BFI shall use a risk-based audit approach to determine the scope, frequency, and intensity of IT audits commensurate with the complexity, sophistication and criticality of technology systems and applications.

10.0.5 (S) An annual IT audit plan shall be developed and approved by the audit committee. The plan shall include key areas for evaluation, audit schedule, and necessary resources to support audit activities.

10.0.6 (S) The BFI shall ensure that IT audit staff possess sufficient information system competency to assess the IT environment and identify the root causes of deficiencies. Alternatively, the BFI may consider utilizing qualified external resources.

10.0.7 (S) The BFI shall ensure that IT audit lead possess professional certifications of IT audit or equivalent with a minimum of three years of IT audit experience, whereas IT audit team members possess at least completion of a comprehensive IT audit training.

10.0.8 (S) The BFI shall provide a continuing education and development for IT audit staff. As the information systems of the BFI become more sophisticated or as more complex technologies evolve, the auditor may need additional training.

10.0.9 (S) The BFI shall establish a standard audit program that includes, but is not limited to, scope, objectives, procedures, and sampling methods.

10.0.10 (S) The BFI shall ensure that IT audit program addresses technology risk exposure areas, which include, but are not limited to, IT asset management, data centers, backup and recovery, incident management, business continuity, access controls, system development, physical security, change management, patch management, data security, network security, system security, vulnerability assessment and penetration testing, and third-party service providers.

10.0.11 (S) The BFI shall establish working papers that include, but are not limited to, scope, objectives, audit period, conclusion, and supporting documentation.

10.0.12 (S) The BFI shall require all audit staff to undergo training on audit programs and working papers before conducting audits. The training shall be provided by experienced auditors or qualified trainers.

10.0.13 (S) The BFI may consider implementing an audit system for managing audit documentation and workflow.

10.0.14 (S) The BFI may consider implementing appropriate computer-assisted audit techniques (CAATs) to perform various audit activities, which include, but are not limited to:

- Testing transactions and balances, such as recalculating interest and conducting analytical reviews; and
- Performing compliance tests of security controls, including setup and configurations of networks and operating systems, as well as vulnerability scans.

10.0.15 (S) The BFI shall ensure that audit findings are communicated clearly and concisely to the auditee, providing detailed information about the identified issues, their potential impact, and recommended corrective actions.

10.0.16 (S) The BFI shall use standardized templates or formats for audit reports to ensure consistency and clarity in presenting audit findings, recommendations, and management responses.

10.0.17 (S) A follow-up process shall be established to track and monitor audit findings.

10.0.18 (S) The BFI shall conduct IT audit quality review to ensure appropriate supervision of IT audit staff with professional due care and free from any conflicts of interest.

10.0.19 (S) The IT audit quality review shall assess the following areas, but not be limited to:

- Audit methodologies, sampling methods, and other substantive procedures
- Evidence collection methods (e.g., observation, inquiry, inspection, interviews, and data analysis) to ensure proper gathering, protection, and preservation of audit evidence;
- Audit quality assurance systems and frameworks; and
- Reporting and communication techniques (e.g., facilitation, negotiation, conflict resolution, audit report structure, issue documentation, management summaries, and result verification).

Appendix

Appendix 1 – Technology Adoption Definition

BFIs utilize various levels of technology. The definition provided below serves as a reference for defining technology adoption based on their sophistication of technology usage, and their nature, size, and complexity. Therefore, the following classifications can be used to identify the technology adoption level of BFIs:

Low:

- Customers need to visit a physical branch for banking services;
- Credit officers provide banking services for loan processing activities to customers at the field through manual process; or
- BFIs use various standalone systems to support banking services, which operate independently without integration with other systems.

Partial:

- Customers need to visit a physical branch for banking services;
- BFIs provide banking service through credit officers for loan processing activities to customers at the field through BFIs' internal application;
- BFIs use various standalone systems to support banking services with some or limited integration with other internal systems;
- BFIs provide limited online services for customer supports; or
- BFIs conduct loan repayment collection and/or payment services via other payment channels as an agent without technology integration.

Medium:

- Customers need to visit a physical branch or ATM for banking services and bill payment services;
- BFIs provide online banking (Internet banking or mobile banking) for balance inquiries, bill payments and/or fund transfers within their own networks and to other BFIs;
- BFIs use various systems to support banking services and intergrate with ATMs and other online payment channels; or
- BFIs conduct loan repayment collection and/or payment services via other payment channels as an agent with real-time integration.

High:

- BFIs provide online banking (Internet banking or mobile banking) for banking services such as fund transfers, bill payments, cross-border payments, and/or new account openings;
- BFIs minimize physical branch visits by providing self-service terminals with a variety of services such as cash deposits and withdrawals, cheque deposits, card services, balance inquiries, fund transfers, bill payments, etc.; or
- BFIs integrate seamlessly with international banking networks to extend online and cross-border payment services.

Advanced:

- BFIs offer comprehensive banking services through mobile banking, internet banking, self-service terminals and/or banking platforms;
- BFIs embrace cutting-edge digital banking technologies with emerging technologies as part of the banking services; or
- BFIs unify the banking experience across channels (mobile, online, and/or in-person) by integrating internal and external services through an omni-channel approach.

Appendix 2 – IT Governance Structure

2.1 Proposed structure for IT governance

Technology Adoption	Advanced and High	Medium	Low and Partial
Committee Structure	Board Risk Committee	Board Risk Committee	Board Risk Committee
	IT Strategy Committee IT Steering Committee Information Security Committee	IT Strategy and Steering Committee Information Security Committee	IT Steering Committee

2.2 Board of Directors

The board should perform the following functions, but not be limited to:

a. Approve and oversee IT-related strategies and policies;
b. Approve a clear risk appetite and tolerance statement defining the nature and extent of technology and cyber risks;
c. Ensure that management has put an effective IT governance process in place;
d. Ascertain that management has implemented processes and practices that ensure that the IT function delivers value to the business;
e. Ensure that IT investments represent a balance of risks and benefits and that budgets are adequate;
f. Maintain continuous improvement program and effective monitoring of technology and cyber risks; and
g. Ensure an independent audit function is established to assess the effectiveness of controls, risk management and governance.

2.3 IT Strategy Committee

The IT Strategy Committee comprises of the following stakeholders:

a. Chief executive officer;
b. Chief or head of operation officer;
c. Chief or head of finance;
d. Chief or head of information technology officer;
e. Chief or head of information security officer; and
f. Other CXOs involved.

The IT strategy committee should perform the following functions, but not be limited to:

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 or plans;
d. Ensure IT organizational structure is defined, which will help in meeting the business needs;
e. Ensure outside expertise is available to the organization as and when required; and

f. Ensure that adequate investments for IT are available for operations and ongoing technology risk management.

It is recommended that the IT strategy committee should have the following powers, but not be limited to:

a. Perform oversight functions over the IT steering committee at a senior management level;
b. Investigate activities within the 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.

2.4 IT Steering Committee

The IT steering committee comprises of the following stakeholders:

a. Representatives from IT team;
b. Representatives from IT security team;
c. Representatives from legal/compliance team;
d. Representatives from HR team;
e. Representatives from the business team; and
f. Other relevant representatives.

IT steering committee assists the executive management in implementing IT strategy that has been approved by the board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including resource conflict), monitoring service levels and improvements, IT service delivery, and IT projects.

The IT steering committee should focus on implementation. Its functions include, but are not limited to:

a. Direct functional leads as designated by the IT strategy committee;
b. Define project prioritizes and assess a 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 monitor key IT governance processes;
e. Advise on infrastructure and products, and provide direction related to technology standards and practices;
f. Ensure that the vulnerability assessment of technologies is performed; and
g. Ensure compliance with regulatory and statutory requirements, standards and guidelines.

2.5 Risk Committee

The Risk Committee comprises of the following stakeholders:

a. Chief risk officer;
b. Chief or head of information officer or technology officer;
c. Chief or head of information security officer; and
d. Other CXOs involved.

The roles and responsibilities of the risk committee shall include, but not be limited to:

- Promote an enterprise risk management competence throughout the BFI, including facilitating the development of IT-related enterprise risk management expertise;
- Ensure that effective risk management practices and internal controls are instituted to achieve data security, system security, reliability, resiliency, and recoverability;
- Establish a common risk management language that includes measures around likelihood and impact, and risk categories;
- Put in place adequate and robust risk management systems as well as operating procedures to manage the risk;
- Implement appropriate practices and controls to mitigate risks and monitor technology risk assessment to include changes in systems, environmental or operational conditions that would affect risk analysis; and
- Ensure that policies and processes are implemented by senior executive in charge of IT operations or chief or head of information officer as defined by the BFI.

2.6 Information Security Committee

The Information security committee comprises of the following stakeholders:

a. Chief or head of information technology officer;
b. Chief or head of information security officer;
c. Chief or head of business or operation; and
d. Other CXOs involved.

The roles and responsibilities of the information security committee shall include, but not be limited to the following functions:

a. Oversee the BFI's information security risk management and operation;
b. Provide guidance and direction on information security, cybersecurity, data protection, and privacy;
c. Ensure compliance with relevant laws, regulations, obligations, and industry standards pertaining to information security; and
d. Seek support from other committees to align information security efforts with overall business goals and strategies.

Appendix 3 – Information Asset Lifecycle

3.1 Roles and Responsibilities

The roles and responsibilities of the information asset management shall be established to include, but are not limited to:

- **Information asset owner:** This is a business executive or business manager who is responsible for each information asset;
- **Information asset custodian:** The information asset custodian is commonly an IT official, who receives delegation from the information asset owner to take responsibility for information security of the information asset such as, maintaining, operating, and disposing;
- **System owner:** The system owner is the manager of the business line who is fully accountable for the performance of the business function served by the system.
- **Security administrator:** The security administrator has the power to set and administer system-wide security controls, user IDs and access rights to information assets. These security administrators usually report to the information security function; and
- **End user:** The end user is any employee, contractor or vendor of BFIs, who uses information systems resources as part of their job.

3.2 Data/Information Classification

Data/Information classification is the process of assigning an appropriate level of classification to BFIs' data/information to ensure it receives an adequate level of protection. The BFI should consider the following criteria for the classification of data/information, but are not limited to, physical, technical, and administrative controls, reproduction, distribution, destruction, and disposal of data/information.

While BFIs can design their own classification, the classification below is a set of widely accepted classification tiers which can consider for data/information classification:

Classification	Explanation
Confidential	This classification applies to the most sensitive or critical business information, which is intended strictly for use within the BFI for the exclusive authorized audience. Its unauthorized disclosure could significantly and adversely impact the BFI's business, shareholders, business partners, and/or its customers, leading to financial, legal, and regulatory repercussions.
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.
Restricted	This classification applies to any sensitive or critical business information which is intended for use within the BFI for a limited set of personnel, but it is not as critical as confidential. Its unauthorized disclosure could adversely impact the 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 the BFI's employee. While its unauthorized disclosure is against policies, it is not expected to seriously or adversely impact the business, shareholders, business partners, employees, and/or customers.
Public	This classification applies to information, which has been explicitly approved by the BFI for release to the public.

mAppendix 4 – Incident Classification

Incident Severity	Definition	Examples
Critical	An incident classified as critical has a high level of impact and causes significant disruption to the BFI's operations and services. It affects the core functions of the business and may severely impact customer services. Such incidents often require immediate attention to prevent further escalation and potential loss of customer trust or revenue.	• Malicious software and hardware attack • Unauthorized access to critical systems • Data breach, leak or loss • Denial of service attacks affecting the critical systems • Outages/degradation of services
Major	An incident classified as major has a medium level of impact and leads to a minimal disruption in the BFI's operations. It might impact a subset of staff or customers, resulting in the temporary loss of the ability to provide a critical service. These incidents require prompt attention to restore normal service levels and minimize downtime.	• System/application failure • Physical security breach • Insider threat • Identity theft • Equipment theft/loss
Minor	An incident classified as minor has a low level of impact and causes no noticeable disruption to the BFI's operations. These incidents may result in a lack of efficiency, but do not generally impede critical services. They can often be resolved through routine troubleshooting and may be addressed during regular maintenance windows.	• Phishing/social engineering • Security Misconfiguration • Unusual network traffic • Failed backup processes

Note: The incident types for each severity level are not necessarily the same as what are mentioned in the above examples. Its severity level depends on the actual impact and materiality caused by each incident.

Appendix 5 – Glossary

Terms	Definitions
Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. *Source: NIST SP 800-27*
Anonymization	Irreversible severance of a data set from the identity of the data contributor to prevent any future reidentification, even by the organization collecting the data under any condition. *Source: ISACA*
Auditability	The level to which transactions can be traced and audited through a system. *Source: ISACA*
Authenticity	The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, a message, or message originator. *Source: NIST SP 800-53, REV. 5*
Authorization	The process of determining if the end user is permitted to have access to an information asset or the information system containing the asset. *Source: ISACA*
Availability	The ability to ensure timely and reliable access to, and use of, information. *Source: ISACA*
Baseline	A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedure. *NIST SP 800-53 Rev. 5*
Black box testing	A testing approach that focuses on the functionality of the application or product and does not require knowledge of the code intervals. *Source: ISACA*
Board	Board of directors of banks and financial institutions.
Business impact assessment	The process of evaluating the criticality and sensitivity of information assets by determining the impact of losing the support of any resource to an enterprise. This establishes the escalation of a loss over time, identifies the minimum resources needed to recover and prioritizes the recovery of processes and the supporting system. Scope Notes: This process captures income loss, unexpected expense, legal issues (regulatory compliance or contractual), interdependent processes and loss of public reputation or public confidence. *Source: ISACA*
Cloud computing	Convenient, scalable on-demand network access to a shared pool of resources that can be provisioned rapidly and released with minimal management effort or service provider interaction. *Source: ISACA*
Confidentiality	Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information. *Source: ISACA*
Corporate governance	Organizational chart, general assembly of shareholders, the board of directors, the board of supervisors and senior managers by assigning clear responsibilities to ensure independent operation and effective check and balance as well as efficient policy-making, incentive and constraint mechanism.

Terms	**Definitions**
	Source: National Bank of Cambodia’s Prokas - B7-011-242 Prokor
Critical function	Business activities or information that cannot be interrupted or unavailable for several business days without significantly jeopardizing operation of the enterprise. *Source: ISACA*
Critical system	A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. *Source: PCI SSC*
Cryptography	The study of mathematical techniques related to aspects of information security, such as confidentiality, data integrity, entity authentication and data origin authentication. *Source: ISACA*
Cyber drill exercise	A simulated attack that replicates real-life scenarios to test an organisation's incident response plans and preparedness. *Source: CM-Alliance*
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report. *Source: ISACA*
Encryption	The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext). *Source: ISACA*
Escrow agreement	A legal arrangement whereby an asset (often money but sometimes other property such as art, a deed of title, website, software source code or a cryptographic key) is delivered to a third party (named an escrow agent) to be held in trust or otherwise pending a contingency or the fulfillment of a condition(s) in a contract. Scope Notes: Upon the occurrence of the escrow agreement, escrow agents will deliver the asset to the proper recipient; otherwise, the escrow agents are bound by their fiduciary duty to maintain the escrow account. Source code escrow signifies a deposit of the source code for the software into an account held by an escrow agent. Escrow is typically requested by a party licensing software (e.g., licensee or buyer) to ensure maintenance of the software. The software source code is released by the escrow agent to the licensee if the licensor (e.g., seller or contractor) files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement. *Source: ISACA*
False acceptance rate	The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. *SOURCE: NIST SP 800-76*
False rejection rate	The probability that a biometric system will fail to identify an applicant or verify the legitimate claimed identity of an applicant. *SOURCE: NIST SP 800-76*
Framework	A framework is a basic conceptual structure used to solve or address complex issues. An enabler of governance. A set of concepts, assumptions and practices that define how something can be approached or understood, the relationships among the entities involved, the roles of those involved and the boundaries

Terms	Definitions
	(what is and is not included in the governance system). *Source: ISACA*
Guideline	A guideline offers recommendations on how standards and baselines are implemented and serves as an operational guide for both security professionals and users. *Source: ISC2 CISSP*
Gray box testing	A test methodology that assumes some knowledge of the internal structure and implementation detail of the assessment object. *Source: NIST SP 800-53A, REV. 5*
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. *SOURCE: NIST SP 800-47, REV. 1*
Infrastructure as a service	A form of cloud computing that offers the capability to provision processing, storage, networks, and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, including operating systems and applications. *Source: ISACA*
Integrity	The guarding against improper information modification or destruction. This includes ensuring information non-repudiation and authenticity. *Source: ISACA*
Masking	A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report. *Source: ISACA*
Multi-factor authentication	A combination of more than one authentication method, such as token and password (or personal identification number [PIN]) or token and biometric device. *Source: ISACA*
Nonrepudiation	The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data, verifiable by a third party. *Source: ISACA*
Privileged user	Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. *Source: ISACA*
Platform as a service	Offers the capability to deploy onto the cloud infrastructure customer-created or acquired applications that are created using programming languages and tools supported by the provider. *Source: ISACA*
Policy	Statements, rules, or assertions that specify the correct or expected behavior of an entity. *Source: NISTIR 7621*
Privacy by design	A guideline to integrate privacy protections into products during the early design phase rather than attempting to tack it on at the end of development. It is effectively the same overall concept as "security by design" or "integrated security," where security is to be an element of design and architecture of a product starting at initiation and being maintained throughout the software development lifecycle (SDLC). *Source: ISC2 CISSP*
Privacy impact assessment	The overall process of identifying, analyzing, evaluating, consulting, communicating, and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information (PII) within the broader risk management framework of an enterprise. *Source: ISACA*
Procedure	A detailed, step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution. *Source: ISC2 CISSP*

Terms	Definitions
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. *Source: ISACA*
Recovery point objective	The earliest point in time that is acceptable to recover data, determined based on the acceptable data loss in case of a disruption in operations. The RPO effectively quantifies the permissible amount of data loss in case of interruption. *Source: ISACA*
Recovery time objective	The amount of time allowed for the recovery of a business function or resource after a disaster occurs. *Source: ISACA*
Role-based access control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals. *SOURCE: NIST SP 800-53*
Secure-by-design	A proactive, security-focused approach to the design, development and deployment of products and services that necessitates a holistic organisational approach to cyber security. Secure-by-Design requires cyber threats to be considered from the outset to enable mitigations through thoughtful design, architecture and security measures. Its core value is to protect consumer privacy and data through designing, developing and delivering products and services with fewer vulnerabilities, and then ensuring security is maintained throughout their life cycle. *Source: Australian Cyber Security Centre*
Security operations centre	A formally recognized function or service responsible for protecting information systems, as well as monitoring, detecting, assessing, and remediating cyber threats and cyber incidents. *Source: Adapted from CPMI-IOSCO and ISACA Full Glossary*
Senior management	A group of key executives overseeing day-to-day management of the institution. *Source: National Bank of Cambodia's Prakas – B7-08-211 Prokor*
Single point of failure	A resource whose loss will result in the loss of service or production. *Source: ISACA*
Service set identifier	A name assigned to a wireless access point that allows stations to distinguish one wireless access point from another. *Source: NISTIR 7621 Rev. 1*
Software as a service	Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based email). *Source: ISACA*
Standard	Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls. They provide a course of action by which technology and procedures are uniformly implemented throughout an organization. *Source: ISC2 CISSP*

Terms	**Definitions**
Tokenization	Tokenization is the use of a token, typically a random string of characters, to replace other data. *Source: ISC2 CISSP*
Two-factor authentication	The use of two independent mechanisms for authentication (e.g., requiring both a smart card and a password), typically the combination of something you know, are or have. *Source: ISACA*
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. *Source: NIST SP 800-53*
Virtual private network	A secure private network that uses the public telecommunications infrastructure to transmit data. *Source: ISACA*
White box testing	A testing approach that uses knowledge of a program/module’s underlying implementation and code intervals to verify its expected behavior. *Source: ISACA*
Web application firewall	A buffer used between a web application and the Internet to mitigate cyberattacks. *Source: ISACA*