Policy Paper issued on the basis of sections 15 and 15a of the State Ordinance on the Supervision of the Credit System (SOSCS).

1. Introduction

The advancement of information technology ("IT") has brought about rapid changes to the way businesses and operations are being conducted in the banking industry. Financial systems and networks supporting banks' business operations have also grown in scope and complexity over the years. In most cases IT is no longer a support function for banks, but a key enabler for business strategies including reaching out to and meeting customer needs. Banks offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers.

Banks are also faced with the challenge of keeping pace with the needs and preferences of consumers who are getting more IT-savvy and switching to internet and mobile devices for financial services, given their speed, convenience and ease of use. Increasingly, banks are deploying more advanced technology and online systems, including internet banking systems, mobile banking and payment systems, to reach their customers. In this regard, banks should fully understand the technology risks arising from these systems. They should also put in place adequate and robust risk management systems as well as operating processes to manage these risks.
The Technology Risk Management Guidelines (the "Guidelines") set out risk management principles and best practice standards to guide banks in the following:

(a) Establishing a sound and robust technology risk management framework;
(b) Deploying strong authentication to protect customer data, transactions and systems; and
(c) Strengthening system security, reliability, resiliency, and recoverability.

The structure of this policy paper is presented in figure 1.

Figure 1. Structure of policy paper

2. Scope and applicability

These Guidelines are based on best practices and should be applied by all credit institutions[1] supervised by the CBA, unless IT is not a core or critical function, or alternative measures have been taken to comply with the objectives of these Guidelines that can be considered equally effective. In this policy paper the deposit-taking credit institutions are referred to as banks. Any deviation from the guidelines contained in this policy paper must be explained in a separate document, to be made available directly to the CBA upon request. In case parts of this policy paper are not applicable, for example if no online banking services are provided, this must also be recorded in the aforementioned document.

1 Reference is made to section 1 of the State Ordinance on the Supervision of the Credit System (AB 1998 No 16).

3. Oversight of Technology Risks by the supervisory board and senior management

IT is a core function at banks. When critical systems fail and customers cannot access their accounts, a bank's business operations may immediately come to a standstill. The impact on customers would be instantaneous, with significant consequences to the bank, including financial and reputational damage.
In view of the importance of the IT function in supporting a bank's business, the supervisory board and senior management should have oversight of technology risks and ensure that the organization's IT function is capable of supporting its business strategies and objectives.

3.1 Roles and Responsibilities

3.1.1 Senior management should ensure that a sound and robust technology risk management framework is established and maintained and should also be involved in key IT decisions.

3.1.2 Senior management is fully responsible for ensuring that effective internal control and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

3.1.3 The Supervisory board should see to it that points 3.1.1 and 3.1.2 are complied with.

3.2 IT Policies, Standards and Procedures

3.2.1 Banks should establish IT policies, standards, and procedures to manage technology risks and safeguard information system assets[2] in the organization in line with current industry standards, approved by Senior Management or a Senior Officer or the bank's board of directors (or an appropriate committee thereof), setting forth the banks' protection of its information systems and nonpublic information stored on those information systems.

3.2.2 Due to rapid changes in the IT operating and security environment, policies, standards, and procedures should be reviewed and updated at least annually.

3.2.3 Compliance processes should be implemented to verify that IT security standards and procedures are enforced. Follow-up processes should be implemented so that compliance deviations are addressed and remedied on a timely basis.

3.2.4 The bank should have a cybersecurity policy based on the bank's risk assessment and address cyber risk threats to the extent applicable to the bank's operations.

2 Information systems assets refer to data, systems, network devices and other IT equipment.

3.3 People Selection Process

3.3.1 Careful selection of staff, vendors and contractors is crucial to minimize technology risks due to system failure, internal sabotage or fraud. As people play an important role in managing systems and processes in an IT environment, banks should implement a screening process that is comprehensive and effective.

3.3.2 Staff, vendors and contractors, who are authorized to access a bank's systems, should be required to protect sensitive or confidential information.

3.4 IT Security Awareness

3.4.1 A comprehensive IT security awareness training program should be established to enhance the overall IT security awareness level within the banking organization. The training program should include information on IT security policies and standards as well as the employee's individual responsibility in respect of IT security and measures that should be taken to safeguard information system assets. Every employee in the organization should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources.

3.4.2 The training program should be conducted and updated at least annually.

3.4.3 The training program should be reviewed and updated where necessary to ensure that the contents of the program remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks.

4. Technology Risk Management Framework

A technology risk management framework should be established to manage technology risks in a systematic and consistent manner. The framework should encompass the following attributes:

(a) Roles and responsibilities in managing technology risks;
(b) Identification and prioritization of information system assets;
(c) Identification and assessment of impact and likelihood of current and emerging threats, risks, and vulnerabilities;
(d) Implementation of appropriate practices and controls to mitigate risks; and
(e) Periodic update of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.

Effective risk management practices and internal controls should be instituted to achieve data confidentiality[3] system security, reliability, resiliency and recoverability in the organization

4.1 Information System Assets

4.1.1 Information system assets should be adequately protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

4.1.2 Banks should establish clear policies on information system asset protection. Criticality of information system assets should be identified and ascertained in order to develop appropriate plans to protect them.

4.2 Risk Identification

4.2.1 Risk identification entails the determination of the threats and vulnerabilities to a bank's IT environment which comprises the internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

4.2.2 A threat may take the form of any condition, circumstance, incident or person with the potential to cause harm by exploiting vulnerability in a system. The source of the threat can be natural, human or environmental. Humans are significant sources of threats through deliberate acts or omissions which could inflict extensive harm to a bank and its information systems.

4.2.3 Security threats such as those manifested in denial of service attacks, internal sabotage and malware infestation, or other form of cyber threat could cause severe harm and disruption to the operations of a bank with consequential losses for all parties affected. Banks should be vigilant in monitoring such risks as it is a crucial step in the risk containment exercise.

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

4.3 Risk Assessment

4.3.1 Following risk identification, banks should perform an analysis and quantification of the potential impact and consequences of these risks on their overall business and operations.

4.3.2 The extent of risk impact depends on the likelihood of various threat and vulnerability pairings or linkages capable of causing harm to the organization should an adverse event occur.

4.3.3 Banks should develop a threat and vulnerability matrix to assess the impact of the threat to their IT environment. Such matrix will also assist in prioritizing IT risks.

4.3.4 Banks should maintain/include a cybersecurity program designed to protect the confidentiality, integrity and availability of the bank's information systems. The cybersecurity program shall be based on the bank's risk assessment and designed to perform the following core cybersecurity functions:

(a) Identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the bank's information systems;
(b) Use defensive infrastructure and the implementation of policies and procedures to protect the bank's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;
(c) Detect cybersecurity events;
(d) Respond to identified or detected cybersecurity events to mitigate any negative effects;
(e) Recover from cybersecurity events and restore normal operations and services; and
(f) Fulfill applicable regulatory reporting obligations.

4.4 Risk Treatment

4.4.1 For each type of risk identified, banks should develop and implement risk mitigation and control strategies that are consistent with the value of the information system assets and the level of risk tolerance.

4.4.2 Risk mitigation entails a methodical approach for evaluating, prioritizing and implementing appropriate risk-reduction controls. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks. In addition, taking insurance cover for various insurable risks, including recovery and restitution costs should be considered.

4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, banks should give priority to threat and vulnerability pairings with high risk ranking which could cause significant harm or impact to a bank's operations. Banks should assess their risk tolerance for damages and losses in the event that a given risk-related event materializes. The costs of risk controls should be balanced against the benefits to be derived.

4.4.4 It is imperative that banks are able to manage and control risks in a manner that will maintain their financial and operational viability and stability. When deciding on the adoption of alternative controls and security measures, banks should also be conscious of costs and effectiveness of the controls with regard to the risks being mitigated.

4.4.5 Banks should refrain from implementing and running a system where the threats to the safety and soundness of their core and critical IT system are insurmountable and the risks cannot be adequately controlled.

4.5 Risk Monitoring and Reporting

4.5.1 Banks should maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. Banks should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks.

4.5.2 To facilitate risk reporting to management, banks should develop IT risk metrics to highlight systems, processes or infrastructure that have the highest risk exposure. An overall technology risk profile of the organization should also be provided to the supervisory board and senior management. In determining the IT risk metrics, banks should consider risk events, regulatory requirements and audit observations.

4.5.3 Risk parameters may shift as the IT environment and delivery channels change. Thus, banks should review and update the risk processes accordingly, and conduct a re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes.

4.5.4 Management of the IT function should review and update its IT risk control and mitigation approach, taking into account changing circumstances and variations in the bank's risk profile.

5. Operational IT Risk Guidelines

Many systems fail because of poor system design and implementation, as well as inadequate testing. Banks should identify system deficiencies and defects at the system design, development and testing phases. Establishing a foundation for IT maturity and IT project management where the focus specifically lies on security requirements, testing of systems and end user development to solidify the IT landscape. Continuous attention on improvement of security measures should be given, also yearly IT audits.

5.1 IT Project Management

5.1.1 In drawing up a project management framework, banks should ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. Banks should clearly define in the project management framework, the roles and responsibilities of staff involved in the project.

5.1.2 Banks should establish a steering committee, consisting of business owners, the development team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

5.1.3 Banks should clearly document project plans for all IT projects. In the project plans, banks should set out clearly the deliverables to be realized at each phase of the project as well as milestones to be reached.

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

5.1.5 Banks should establish management oversight of the project to ensure that milestones are reached and deliverables are realized in a timely manner. Banks should escalate issues or problems which could not be resolved at the project committee level to senior management for attention and intervention.

5.2 Security Requirements and Testing

5.2.1 Banks should clearly specify security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling in the early phase of system development or acquisition.

5.2.2 A methodology for system testing[4] should be established. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

4 System testing is broadly defined to include unit, modular, integration, system and user acceptance testing.

5.2.3 Banks should ensure that appropriate testing is performed based on the risk of the system changes being deployed. This includes full regression testing for major systems. Users whose systems and operations are affected by the system changes should review and sign off on the outcome of the tests.

5.2.4 Banks should conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces. In the case that a Bank deviates from this decision, banks should document exceptions properly and have them available to the CBA upon request. In case no prior penetration testing is possible, penetration testing should be performed within a reasonable timeframe, explained and documented. Banks should also perform continuous vulnerability scanning of external and internal network components that support the changed and current system landscape.

5.3 End User Development

5.3.1 There are common business application tools and software which allow business users to develop simple applications to automate their operations, perform data analysis and generate reports for the bank and customers. Banks should perform an assessment to ascertain the importance of these applications to the business.

5.3.2 Recovery measures, user access and data protection controls, at the minimum, should be implemented for such applications.

5.3.3 Banks should review and test based on their risk assessment end user developed program codes, scripts and macro's before they are used so as to ensure the integrity and reliability of the applications.

5.4 IT Audit

5.4.1 As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for banks to develop effective internal control systems to manage technology risks.

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

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

5.5 Audit Planning and Remediation Tracking

5.5.1 Banks' should ensure that the scope of IT audit is comprehensive and includes all critical IT operations. An IT audit plan, comprising auditable IT areas for the coming year, should be developed. The IT audit plan should be approved by Senior Management and the Supervisory Board.

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

6. IT Service Management

A robust IT service management framework is essential for supporting IT systems, services and operations, managing changes, incidents and problems as well as ensuring the stability of the production IT environment. The framework should comprise the governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management, program migration and managing of (privileged) user access onto the IT landscape

6.1 Change Management

6.1.1 Banks should establish a change management process to ensure that changes to production systems are assessed, approved, implemented, and reviewed in a controlled manner.

6.1.2 The change management process should apply to changes pertaining to system and security configurations, patches for hardware devices and software updates.

6.1.3 Prior to deploying changes to the production environment, banks should perform a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems. Banks should also determine if the introduced change would spawn security implications or software compatibility problems to affected systems or applications.

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

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

6.1.6 To minimize risks associated with changes, banks should perform backups of affected systems or applications prior to the change. Banks should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. Banks should establish alternative recovery options to address situations where a change does not allow a bank to revert to a prior status.

6.1.7 Audit and security logs are useful information which facilitates investigations and troubleshooting. Banks should ensure that the logging facility is enabled to record activities that are performed during the migration process.

6.2 Program Migration

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

6.2.2 Banks should separate physical or logical environments for systems development, testing (e.g. user acceptance testing), staging, and production.

6.2.3 Banks should closely monitor vendor and developers' access to all their environments.

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

6.2.5 Segregation of duties should be enforced in so far possible so that no single individual has the ability to develop, compile, and move object codes from one environment to another. In cases where segregation of duties is not completely possible, banks should document and explain this process.

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

6.3 User Access Management

6.3.1 Banks should only grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. Banks should ensure that the resource owner duly authorizes and approves all requests to access IT resources.

6.3.2 Employees of vendors or service providers, who are given authorized access to banks critical systems and other computer resources, pose similar risks as internal staff. Banks should subject these external employees to close supervision, monitoring and access restrictions similar to those expected of its own staff.

6.3.3 For accountability and identification of unauthorized access, banks should ensure that records of user access are uniquely identified and logged for audit and review purposes.

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

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

6.3.6 Banks should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. Banks should also ensure that

any person who needs to access backup files or system recovery resources is duly authorized for a specific reason and a specified time only.

6.4 Privileged Access Management

6.4.1 Information security ultimately relies on trusting a small group of skilled staff, who should be subject to proper checks and balances. Their duties and access to systems resources should be placed under close scrutiny. Banks should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions, taking into account insider threat.

6.4.2 Banks should adopt the following controls and security practices:

(a) Implement strong authentication mechanisms such as two-factor authentication where possible for privileged users;
(b) Institute strong controls over remote access by privileged users;
(c) Restrict the number of privileged users;
(d) Grant privileged access on a "need-to-have" basis;
(e) Maintain audit logging of system activities performed by privileged users;
(f) Disallow privileged users from accessing systems logs in which their activities are being captured;
(g) Review privileged users' activities on a timely basis;
(h) Prohibit sharing of privileged accounts;
(i) Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
(j) Protect backup data from unauthorized access.

6.5 Incident Management

6.5.1 An IT incident occurs when there is an unexpected disruption to the standard delivery of IT services. Banks should appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of IT services or further aggravation.

6.5.2 Banks should establish an incident management framework with the objective of restoring normal IT service as quickly as possible following the incident, and with minimal impact to the bank's business operations. The banks should also establish the roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating, and monitoring incidents.

6.5.3 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, banks may delegate the function of determining and assigning incident severity levels to a centralized technical helpdesk function. Banks should train helpdesk staff to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.

6.5.4 Banks should establish corresponding escalation and resolution procedures where the resolution timeframe is commensurate with the severity level of the incident. The

predetermined escalation and response plan for security incidents[5], should be tested on a regular basis.

6.5.5 Banks should form a computer emergency response team, comprising staff with the necessary technical and operational skills to handle major incidents.

6.5.6 In some situations, major incidents (in terms of cost, image, number of clients affected) may develop into a crisis. Senior management should be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis. Banks should inform the CBA promptly if a major incident occurs with due regard of the requirements as stipulated in guidelines and papers on Sound Business Operations.

6.5.7 Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of a bank. Banks should include in their incident response procedures a predetermined action plan to address public relations issues.

6.5.8 Banks should keep customers informed of any major incident or data breach where their data has potentially been compromised. They should also assess the effectiveness of the mode of communication, including informing the general public, where necessary.

6.5.9 As incidents may stem from numerous factors, banks should perform a root cause and impact analysis for major incidents which result in severe disruption of IT services. Banks should take remediation actions to prevent the recurrence of similar incidents and security breaches.

6.5.10 Banks should include in their incident report an executive summary of the incident, an analysis of root cause which triggered the event, its impact as well as measures taken to address the root cause and consequences of the event.

6.5.11 Banks should adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution. Each bank should notify the CBA as promptly as possible but in no event later than 48 hours in line with the Practices of Sound Business Operations Article 13 in the event that a security breach or major incident has occurred.

6.5.12 Cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the bank should also be reported. Annually each Bank should revise their Cybersecurity program where it has identified areas, systems or processes that require material improvement, updating or redesign. The banks should document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the CBA.

5 Examples of security incidents include virus outbreak, malware infiltration, systems hacking, account impersonation or compromise, phishing attack, internal sabotage or denial of service attacks.

7. Operational Infrastructure Security Management

The IT landscape is vulnerable to various forms of cyber attacks[6] and the frequency and malignancy of attacks are increasing. It is imperative that banks implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats.

Appropriate technological measures should be implemented to protect sensitive or confidential information such as customer personal, account and transaction data which are stored and processed in systems. Customers should be properly authenticated before access to online transaction functions and, sensitive personal or account information is permitted. Sensitive customer information including login credentials, passwords and personal identification numbers (PINs) should be secured against exploits such as ATM skimming, hacking, phishing and malware.

7.1 Data Loss Prevention

7.1.1 Internal sabotage, clandestine espionage or furtive attacks by trusted staff, contractors and vendors are potentially among the most serious risks that banks could face in an increasingly complex and dynamic IT environment. Current and past staff, contractors, vendors and those who have knowledge of the inner workings of a bank's systems, operations and internal controls have a significant advantage over external attackers. A successful attack not only jeopardizes customer confidence in a bank's internal control systems and processes but also causes real financial loss when proprietary information is divulged. Banks should identify important data and adopt adequate measures to detect and prevent unauthorized access, copying or transmission of confidential information.

7.1.2 Banks should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information, taking into consideration the following:

a) Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile devices;
b) Data in motion - Data that traverses a network or that is transported between sites; and
c) Data at rest - Data in computer storage which includes files stored on servers, databases, backup media and storage platforms.

7.1.3 To achieve security of data at endpoints, banks should implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations, and call centers. Banks should protect confidential information stored in all types of endpoint devices with strong encryption.

7.1.4 Banks should not use unsafe internet services such as social media sites or internet storage sites to communicate or store confidential information. Banks should implement measures to manage and detect the use of such services within its organization.

7.1.5 For the purpose of exchanging confidential information with external parties, banks should take utmost care to preserve the confidentiality of information. For this purpose, banks should

6 Cyber attacks include phishing, denial of service attacks, spamming, sniffing, spoofing, hacking, keylogging, phishing, middleman interception, and other malware attacks from mutating virus and worms.

at all times take appropriate measures including sending information through encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length. Banks should send the encryption key via a separate transmission channel to the intended recipients. Alternatively, banks may choose other secure means to exchange confidential information with its intended recipients.

7.1.6 Confidential information stored on IT systems, servers, and databases should be encrypted and protected through strong access controls, bearing in mind the principle of "least privilege"[7].

7.1.7 Banks should assess various methods in which data could be securely removed from the storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems. In determining the appropriate media sanitization method to use, banks should take into consideration security requirements of the data residing on the media.

7.2 Data Backup Management

7.2.1 Banks should develop a data backup strategy for the storage of critical information.

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

7.2.3 Banks should carry out periodic testing and validation of the recovery capability of backup media and assess if the backup media is adequate and sufficiently effective to support the recovery process.

7.2.4 Banks should encrypt backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.

7.3 Technology Refresh Management

7.3.1 To facilitate the tracking of IT resources, banks should maintain an up-to-date inventory of software and hardware components used in the production and disaster recovery environments which includes all relevant associated warranty and other support contracts related to the software and hardware components.

7.3.2 Banks should actively manage their IT systems and software so that outdated and unsupported systems which significantly increase its exposure to security risks are replaced on a timely basis. Banks should pay close attention to the product's end-of-support ("EOS") date as it is

7 Least privilege is defined as assigned privileges on a "need-to-have" basis.

common for vendors to cease the provision of patches, including those relating to security vulnerabilities that are uncovered after the product's EOS date.

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

7.4 Networks and Security Configuration Management

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

7.4.2 Banks should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

7.4.3 Banks should deploy anti-virus software to servers, if applicable, and workstations. Banks should regularly update anti-virus definition files and schedule automatic anti-virus scanning on servers and workstations on a regular basis.

7.4.4 Banks should install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical junctures of their IT infrastructure to protect the network perimeters. Banks should deploy firewalls, or other similar measures, within internal networks to minimize the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network. On an annual basis, banks should also back up and review rules on network security devices to determine that such rules are appropriate and relevant.

7.4.5 Banks deploying Wireless Local Area Networks (WLAN) within the organization should be aware of the risks associated herewith. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorized access.

7.5 Vulnerability Assessment and Penetration Testing

7.5.1 Systems Vulnerability Assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. Banks should conduct VAs regularly to detect security vulnerabilities in the IT environment.

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

7.5.3 Banks should establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

7.5.4 Banks should carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. Banks should conduct penetration tests on internet-facing systems at least annually and full scope penetration tests at least once every two years.

7.6 Patch Management

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

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

7.7 Security Monitoring

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

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

7.7.3 Banks should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes. Banks should include capacity management to support business functions, and ensure that indicators such as performance, capacity, and utilization are monitored and reviewed.

7.7.4 Banks should perform real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications.

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

7.7.6 Banks should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, banks should take into account statutory requirements for document retention and protection.

7.8 Data Center protection

7.8.1 As banks' critical systems and data are concentrated and maintained in the Data Center (DC), it is important that the DC is resilient and physically secured from internal and external threats.

7.8.2 The purpose of a physical Threat and Vulnerability Risk Assessment (TVRA) is to identify security threats to and operational weaknesses in a DC in order to determine the level and type of protection that should be established to safeguard it. A bank should base its TVRA on various possible scenarios of threats which include theft, explosives, arson, unauthorized entry, external attacks and insider sabotage.

7.8.3 Banks should include in the scope of the TVRA a review of the DC's perimeter and surrounding environment, as well as the building and DC facility. Banks should also review daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls.

7.8.4 When selecting a DC provider, banks should obtain and assess the TVRA report on the DC facility. Banks should verify that TVRA reports are current and that the DC provider is committed to address all material vulnerabilities identified. For banks that choose to build their own DC, an assessment of threats and vulnerabilities should be performed at the feasibility study stage.

7.8.5 Banks should limit access to DC to authorized staff only. Banks should only grant access to the DC on a need to have basis. Physical access of staff to the DC should be revoked immediately if it is no longer required. Banks should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the DC. Banks should establish physical security measures to prevent unauthorized access to systems, equipment racks and tapes.

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

7.8.7 Banks should ensure that the perimeter of the DC, DC building, facility, and equipment room are physically secured and monitored. Banks should employ physical, human and procedural controls (e.g. security guards, card access systems, mantraps and bollards) where appropriate.

7.9 Data Centre Resiliency

7.9.1 To achieve DC resiliency, banks should assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications.

7.9.2 Banks should rigorously control and regulate the environment within a DC. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical in ensuring uptime and system reliability. Banks should promptly escalate any abnormality detected to management and resolve the abnormality in a timely manner.

7.9.3 Banks should implement appropriate fire protection and suppression systems in the DC to control a full scale fire if it occurs. Banks should install smoke detectors and hand-held fire extinguishers in the DC and implement passive fire protection elements, such as fire walls around the DC, to restrict the spread of a fire to a portion of the facility.

7.9.4 To ensure there is sufficient backup power, banks should install backup power consisting of uninterruptible power supplies, battery arrays, and/or diesel generators.

8. Online Financial Services[8]

Whilst the internet presents opportunities for banks to reach new markets and expand its range of products and services, being an open network, it also brings about security risks that are more sophisticated and dynamic than closed networks and proprietary delivery channels. Banks should be cognizant of risks that are brought about as a result of offering financial services via the internet platform.

There are varying degrees of risks associated with different types of services provided over the internet. Typically, financial services offered via the internet can be classified into information service[9], interactive information exchange service[10] and transactional service[11]. The highest level of risk is associated with transactional service as online transactions are often irrevocable once executed.

Banks should clearly identify risks associated with the types of services being offered in the risk management process. Banks should also formulate security controls, system availability and recovery capabilities, which are commensurate with the level of risk exposure, for all internet operations.

8.1 Online Systems Security

8.1.1 Banks should devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

8.1.2 Banks should provide their customers and users of their internet services the assurance that online login access and transactions performed over the internet on their websites are adequately protected and authenticated.

8.1.3 The CBA expects banks to properly evaluate the security requirements associated with their internet systems and adopt encryption algorithms, with due regard of the international standards in this area (e.g. PCI-DSS, ISO, NIST).

8.1.4 Banks should ensure that information processed, stored or transmitted between their bank and their customers is accurate, reliable and complete. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. Banks' should implement physical and logical access security to allow only authorized staff to access its systems. Banks should also implement appropriate processing and transmission controls to protect the integrity of systems and data.

8.1.5 Banks should implement monitoring or surveillance systems so that it is alerted to any abnormal system activities[12], transmission errors or unusual online transactions. Banks should

8 Online financial services refer to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices.

9 Information service is the most basic form of online internet service. It is a one-way communication whereby information, advertisements or promotional material are provided to the customers.

10 Interactive information exchange service allows customers to communicate with the FI, make account enquiries and fill in application forms to take up additional services or purchase new products offered.

11 Transactional service allows customers to execute online transactions such as the transfer of funds, payment of bills and other financial transactions.

12 An example of the abnormal system activities includes multiple sessions using an identical customer account originating from different geographical locations within a short time span.

establish a follow-up process to verify that these issues or errors are adequately addressed subsequently.

8.1.6 Banks should maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). Banks should put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

8.1.7 Banks should implement two-factor authentication[13] at login for all types of online financial systems and transaction-signing for authorizing transactions. The primary objectives of two-factor authentication and transaction-signing are to secure the customer authentication process and to protect the integrity of customer account data and transaction details as well as to enhance confidence in online systems by combating cyber attacks targeted at banks and their customers.

8.1.8 Banks should also take appropriate measures to minimize exposure to other forms of cyber attacks such as middleman attack which is more commonly known as a man-in-the-middle attack[14] (MITMA), man-in-the browser attack or man-in-the application attack.

8.1.9 As more customers log onto banks' websites to access their accounts and conduct a wide range of financial transactions for personal and business purposes, banks should put in place measures to protect customers who use online systems. In addition, banks should educate its customers on security measures that are put in place to protect their customers in an online environment.

8.2 Mobile Online Services and Payments Security

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

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

13 Two-factor authentication for system login can be based on any two of the factors, i.e. What you know (e.g. PIN), what you have (e.g. OTP token) and who you are (e.g. Biometrics).

14 In a man-in-the-middle attack, an interloper is able to read, insert and modify messages between two communicating parties without either one knowing that the link between them has been compromised. Possible attack points for MITMA could be customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the customer and the FI's server.

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

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

8.3 Payment Card Security (ATM's, Credit and Debit Cards)

8.3.1 Payment cards[15] allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase their items over the internet, or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines (ATMs) or conducting payments at point of sales (POS) located at merchants.

8.3.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Banks should follow international standards of migrating away from magnetic stripe card types to other, safer, methods (e.g. EMV chip supported card transactions).

8.3.3 Types of payment card fraud include counterfeit, lost/stolen, card-not received[16] ("CNR") and card-not-present[17] ("CNP") fraud. Banks should monitor payments patterns for insider threat.

8.4 Payment Card Fraud

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

8.4.2 Banks should deploy secure methods to store sensitive payment card data. Banks should also implement strong card authentication methods such as dynamic data authentication ("DDA") or combined data authentication ("CDA") methods for online and offline card transactions. For interoperability reasons, where transactions could only be effected by using information from the magnetic stripe on a card, banks should ensure that adequate controls are implemented to manage these transactions.

8.4.3 Banks card issuer, and not a third party payment processing service provider, should perform the authentication of customers' sensitive static information, such as PINs or passwords.

15 For the purpose of this document, "payment cards" refer to ATM, credit, charge and debit cards.
16 Card-not-received fraud refers to fraud cases where cardholders do not receive cards dispatched by the issuing banks and subsequently, these cards are used to make fraudulent transactions.
17 Card-not-present fraud involves the use of stolen or compromised card details to make purchases over the internet, phone or mail order.

Banks should perform regular security reviews of the infrastructure and processes being used by their service providers and merchants.

8.4.4 Banks should ensure that security controls are implemented at payment card systems and networks.

8.4.5 To enhance card payment security, banks should promptly notify cardholders via transaction alerts when withdrawals / charges exceeding customer-defined thresholds are made on the customers' payment cards. Banks should implement robust fraud detection systems with behavioral scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities. Banks should set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

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

8.5 ATMs and Payment Kiosks Security

8.5.1 The presence of ATMs and payment kiosks have provided cardholders with the convenience of withdrawing cash as well as making payments to billing organizations. However, these systems are targets where card skimming attacks are perpetrated.

8.5.2 To secure consumer confidence in using these systems, banks should put in place the following measures to counteract fraudsters' attacks on ATMs and payment kiosks:

(a) Install anti-skimming solutions on these machines and kiosks to detect the presence of foreign devices placed over or near a card entry slot;
(b) Install detection mechanisms and send alerts to appropriate staff at bank for follow-up response and action;
(c) Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission;
(d) Implement appropriate measures to prevent shoulder surfing of customers' PINs; and
(e) Conduct video surveillance of activities at these machines and kiosks; and maintain the quality of CCTV footage.

8.5.3 Banks should verify that adequate physical security measures are implemented at third party payment kiosks, which accept and process banks' payment cards.

9. Systems Reliability, Availability and Recoverability

The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capabilities of a bank. When critical systems fail, the disruptive impact on the bank's operations or customers will usually be severe and widespread and the bank may suffer serious consequences to its reputation. The Policy Paper on Business Continuity Management (BCM) contains the complete organizational structure set out to aid the BCM cycle. This section emphasizes the technological aspects when setting up and preparing a Disaster Recovery Plan.
As all systems are vulnerable, banks should define their recovery and business resumption priorities. A bank should also regularly test its contingency procedures in line with the Policy Paper on Business Continuity Management in order to minimize disruptions of its business arising from a serious incident.

9.1 Systems Availability

9.1.1 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability, and swift recovery capability. Banks should ensure that the business continuity plans are updated and that the recovery site can support the new production environment.

9.1.2 Banks may employ a number of complex interdependent systems and network components for their IT processing. An entire system can become inoperable when a single critical hardware component or software module malfunctions or is damaged. Banks should develop built-in redundancies to reduce single points of failure which can bring down the entire network. Banks should include a strategy to have standby hardware, software and network components that are necessary for their recovery.

9.1.3 Banks should achieve high availability[18] for critical systems[19].

9.2 Disaster Recovery Plan

9.2.1 In formulating and constructing a rapid recovery plan, banks should include a scenario analysis to identify and address various types of contingency scenarios. Banks should plan for the recovery from at least the following disruptive events:

(a) Natural events such as hurricanes, floods, other severe weather conditions;
(b) Technical events such as power outage and fluctuations, communication failure, equipment and software failure; banks should consider scenarios such as major system outage, which may be caused by system faults, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary DC.
(c) Malicious activities including network security attacks, frauds, assaults and public riots; and
(d) Fires.

18 Other than during periods of planned maintenance, banks should enhance their systems and infrastructure resiliency by deploying suitable solutions, e.g., active-active setup, for these systems to minimize downtime.
19 Critical system means a system, the failure which will cause significant disruption to the operations of a bank or materially impact the bank's service to its customers. "System" means any hardware, software, network or IT component which is part of an IT infrastructure

9.2.2 IT incidents, if handled inappropriately, may escalate into situations that have a severe impact on banks' operations or its customers. Banks should evaluate their recovery plan and incident response procedures at least annually and update them as and when changes to business operations, systems and networks occur.

9.2.3 To strengthen recovery measures relating to large-scale disruptions and to achieve risk diversification, banks should implement adequate backup and recovery capabilities at the individual system or application cluster level. Banks should consider inter-dependencies between critical systems in drawing up their recovery plan and conducting contingency tests.

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

9.2.5 Insofar the size of the institution allows so, banks should establish a recovery site that is sufficiently outside perimeter of primary site to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site.

9.2.6 The required speed of recovery will depend on the criticality of resuming business operations, the type of services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers. Banks may wish to explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance their recovery capability.

9.2.7 The resiliency and robustness of critical systems which are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links. To minimize impact on business operations in the event of a disruption, banks should ensure cross-border network redundancy, insofar as possible.

9.3 Disaster Recovery Testing

9.3.1 During a system outage, banks should refrain from adopting impromptu and untested recovery measures over pre-determined recovery actions that have been rehearsed and approved by management. Ad hoc recovery measures carry high operational risks as their effectiveness has not been verified through rigorous testing and validation.

9.3.2 Banks should test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

9.3.3 Banks should test the recovery dependencies between systems. Bilateral or multilateral recovery testing should be conducted where networks and systems are linked to specific service providers and vendors.

9.3.4 Banks should involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly. Banks should also participate in disaster recovery tests that are conducted by its service provider(s), including those systems which are located offshore.

10. MANAGEMENT OF IT OUTSOURCING RISKS

IT outsourcing comes in many forms. Some of the most common types of IT outsourcing are in systems development and maintenance, support to DC operations, network administration, disaster recovery services, application hosting, and cloud computing. Outsourcing can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Aruba or abroad. The supervisory board and senior management should fully understand the risks associated with IT outsourcing. Reference is made to Policy Paper IV.10 Outsourcing Arrangements issued by the CBA.

10.0.1 Banks should require the service provider to implement security policies, procedures, and controls that are at least as stringent as they would expect for their own operations.

10.0.2 All parties concerned, including those from the service provider, should receive regular training in activating the contingency plan and executing recovery procedures.

10.0.3 Banks should have contingency plans in place based on credible worst case scenarios for service disruptions to prepare for the possibility that their current service provider may not be able to continue operations or render the services required. The plan should incorporate identification of viable alternatives for resuming the IT operations elsewhere.