BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 808
Series of 2013

Subject: **Guidelines on Information Technology Risk Management for All Banks and Other BSP Supervised Institutions**

The Monetary Board, in its Resolution No. 1286 dated 01 August 2013, approved the amendments to Sections X176 and X705 of the Manual of Regulations for Banks (MORB) to enhance the guidelines on information technology risk management.

Section 1. Technology Risk Management. §X176 and the related Appendix 75 of the Manual of Regulations for Banks (MORB) are hereby amended to read as follows:

§X176. Information Technology Risk Management (ITRM). The enhanced guidelines on ITRM keep abreast with the aggressive and widespread adoption of technology in the financial service industry and consequently strengthen existing BSP framework for IT risk supervision. ITRM should be considered a component and integrated with the institutions' risk management program. The guidelines likewise provide practical plans to address risks associated with emerging trends in technology and growing concerns on cyber security.

§X176.1 ***Declaration of Policy.*** A growing number of BSP supervised institutions (BSIs) employ the advances in technology as leverage to offer innovative products, deliver fast and efficient service at affordable prices, and venture to new markets. Moreover, technology drives the efficiency of operations and financial accounting of these institutions, and improves their decision-making process. As technology becomes an integral part of the business and operations of BSIs, such technology usage and dependence, if not properly managed, may heighten technology risks. The BSP expects BSIs to have the knowledge and skills necessary to understand and effectively manage technology risks. These institutions are required to have an integrated approach to risk management to identify, measure, monitor and control risks.

§X176.2 ***Purpose and Scope.*** The enhanced guidelines aim to provide guidance in managing risks associated with use of technology. The guidelines outlined in this Circular are based on international standards and recognized principles of international practice for ITRM and shall serve as BSP's baseline requirement for all BSIs.

The guidelines shall apply to BSIs which include banks, non-banks with quasi-banking function (NBQB), non-bank electronic money issuers and other non-bank institutions which under existing BSP rules and regulations and special laws are subject to BSP supervision and/or regulation. Moreover, subject guidelines shall also apply to BSIs with offshore data processing as may be appropriate to their situation. The framework covers different facets of ITRM, some of which are supplemented with detailed guidelines in the attached Appendices. The BSP shall keep the Appendices updated and, in the future,

issue additional regulations on new and emerging products, services, delivery channels, and other significant applications of technology.

Subject guidelines (including the attached Appendices) are not "one-size-fits-all" and implementation of these need to be risk-based and commensurate with size, nature and types of products and services and complexity of IT operations of the individual BSIs. BSIs shall exercise sound judgment in determining applicable provisions relevant to their risk profile.

§X176.3 ***Complexity of IT Risk Profile.*** The BSP shall risk profile all BSIs and classify them as either "Complex" or "Simple". The assessment of complexity of IT risk profile is based largely on the degree of adoption of technology and considers size, nature and types of products and services and complexity of IT operations among the risk factors. In assessing IT operations, the nature of IT organization, degree of automation of core processes and applications and extent and reach of online branch network are likewise considered.

A BSI with "Complex" IT risk profile is highly dependent on technology. IT components are integral to the core business activities that major weaknesses on IT systems, maintenance and support, if not properly addressed, may cause operational inefficiencies, business disruptions and/or financial losses. On the other hand, a BSI with "Simple" IT risk profile relies or depends less on technology in the operations of its business, thus, is not affected or lowly impacted by IT-related risks.

However, to facilitate classification, a thrift, rural or cooperative bank shall be deemed as a simple BSI, while universal and commercial banks, which generally have more complex types of products and services, shall be deemed as complex BSIs. Nonetheless, a universal or commercial bank may apply with the BSP for a reclassification as simple BSI in order to avail of reduced compliance with the provisions of subject Circular. The BSP may likewise declare a thrift, rural or cooperative bank as complex based on the assessment of the BSIs IT profile report (pursuant to Subsection X176.8) and other internal supervisory tools. Said banks shall receive notification in writing from the BSP informing them of the deviation from the default classification and the basis for classifying them as complex BSIs.

Non-bank institutions which under existing BSP rules and regulations and special laws are subject to BSP supervision/regulation shall likewise be notified in writing of their classification immediately upon effectivity of this Circular.

§X176.4 ***IT Rating System.*** The BSP, in the course of its on-site examination activities, shall evaluate BSIs' ITRM system and measure the results based on BSP's IT rating system. A composite rating is assigned based on a "1" to "4" numerical scale, as follows:

4	BSIs with this rating exhibit strong performance in every respect. Noted weaknesses in IT are minor in nature and can be easily corrected during the normal course of business.
3	BSIs with this rating exhibit satisfactory performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes or system development.

2	BSIs with this rating exhibit less than satisfactory performance and require considerable degree of supervision due to a combination of weaknesses that may range from moderate to severe.
1	BSIs with this rating exhibit deficient IT environment that may impair the future viability of the entity, thereby requiring immediate remedial action.

The detailed guidelines covering the BSP's IT Rating System shall be issued separately.

§X176.5 ***Definition of Terms.*** In these guidelines, terms are used with the following meanings:

Terminology	Definitions
Board of Directors (Board)	The governing body elected by the stockholders that exercises the corporate powers of a locally incorporated BSI. In case of a BSI incorporated or established outside the Philippines, this may refer to the functional oversight equivalent such as the Country Head (for foreign banks) or management committee or body empowered with oversight and supervision responsibilities.
Cyberfraud	A deliberate act of omission or commission by any person carried out using the Internet and/or other electronic channels, in order to communicate false or fraudulent representations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions connected with the perpetrator. Examples of cyberfraud in the financial industry may include, but are not limited to, theft of credit card data, computer hacking, electronic identity theft, phishing scams, ATM skimming and non-delivery of merchandise purchased online, among others.
Electronic Products and Services	The delivery of banking and financial products and services through electronic, interactive communication channels which include automated teller machines (ATMs), point of sale (POS) terminals, internet, mobile phones, touch tone telephones and other similar electronic devices. These encompass electronic banking, electronic payments, electronic money and other electronic products and services offered by BSIs.
EMV (stands for Europay, MasterCard and Visa)	It is a global standard for credit, debit and prepaid payment cards based on chip card technology. EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.
Encryption	A data security technique used to protect information from unauthorized inspection or alteration. Information is

Terminology	Definitions
	encoded so that data appears as meaningless string of letters and symbols during delivery or transmission. Upon receipt, the information is decoded using an encryption key.
Enterprise-wide Level	Extending throughout or involving an entire institution rather than a single business department or function. In this document, the words "enterprise-wide" and "organization-wide" are interchangeably used.
Information Assets/ Resources	Encompass people and organization, IT processes, physical infrastructure (i.e. facilities, equipment), IT infrastructure (including computing hardware, network infrastructure, middleware) and other enterprise architecture components (including information, applications).
Information Security	The protection of information assets from unauthorized access, use, disclosure, disruption modification or destruction in order to provide confidentiality, integrity and availability.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening the confidentiality, integrity or availability of BSI's information or information systems
Information Technology (IT)	Automated means of originating, processing, storing and communicating information and covers recording devices, communications network, computer systems (including hardware and software components and data) and other electronic devices.
IT Group/Department	The unit of an organization within a BSI responsible for the activities of IT operations control, monitoring of IT services, infrastructure support and a combination of technology, people and processes.
IT Operations	Encompasses all processes and services that are provisioned by an IT Unit to internal and external clients.
IT Outsourcing	An arrangement under which another party (either an affiliated entity within a corporate group or an entity external to the corporate group) undertakes to provide to a BSI all or part of an IT function or service. A BSI would use IT outsourcing for functions ranging from infrastructure to software development, maintenance and support. The related IT service is integral to the provision by BSI of a financial service and the BSI is dependent on the service on an ongoing basis.
IT Risk	Any potential adverse outcome, damage, loss, violation, failure or disruption associated with the use of or reliance on computer hardware, software, devices, systems, applications and networks.
IT Strategic Plan	A long-term plan (i.e., three- to five-year horizon) in which

Terminology	Definitions
	business and IT management cooperatively describe how IT resources will contribute to the institution's strategic objectives.
IT Risk Management System (ITRMS)	Risk management system that enables a BSI to identify, measure, monitor and control IT-related risks
Management Information System (MIS)	A general term for the computer systems in an institution that provide information about its business operations.
Network	Two or more computer systems that are grouped together to share information, software and hardware.
Offshore BSIs	Have their critical system processing and data located outside of the Philippines. These are usually maintained and operated by organizations within the same business group that the BSIs belong to, such as their head office, subsidiary and/or affiliate. Locally-maintained systems, if any, are limited to non-core supporting applications such as collaboration systems and report processing tools.
Project Management	Planning, monitoring and controlling an activity.
Senior Management/ Management	Officers of the institution given the authority by the Board to implement the policies it has laid down in the conduct of the business of the institution.
Service Level Agreement	Establishes mutual expectations and provide a baseline to measure IT performance. An SLA should contain, among others, the specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as it relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee.
Triple Data Encryption Standard (3DES)	A mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

§X176.6 ***Description of IT-Related Risks.*** As BSIs increase their reliance on IT to deliver products and services, inappropriate usage of IT resources may have significant risk exposures. While IT does not trigger new types of risks, it brings in new dimensions to traditional banking risks (i.e. strategic risk, credit risk, market risk, liquidity risk and operational risk) that require new or enhanced control activities (e.g. a failure of a credit risk measurement application is an IT failure and, therefore, a systems failure in the sense of operational risk). Moreover, IT is an implied part of any system of internal controls, regardless of the type of risk and, consequently, forms an important element in organization-wide risk management. Among the risks associated with the use of IT are the following:

1. *Operational risk* is the risk to earnings and capital arising from problems with service or product delivery. This risk is a function of internal controls, IT systems, employee integrity and operating processes. Operational risk exists in all products and services;

2. *Strategic risk* is the risk to earnings and capital arising from adverse business decisions on IT-related investments or improper implementation of those decisions. The risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible which include communication channels, operating systems, delivery networks and managerial capacities and capabilities;

3. *Reputation risk* is the risk to earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. The risk can expose the institution to litigation, financial loss or damage to its reputation; and

4. *Compliance risk* is the risk to earnings and capital arising from the violations of, or non-conformance with laws, rules and regulations, prescribed practices or ethical standards. Compliance risk also arises in situations where the laws and rules governing certain products activities of the BSI's clients may be ambiguous or untested. Compliance risk exposes the institution to monetary penalties, non-monetary sanctions and possibility of contracts being annulled or declared unenforceable.

§X176.7 *IT Risk Management System (ITRMS).* As BSIs become more dependent on IT systems and processes, technology risks and information security issues have become progressively more complex and pressing in recent years. Information security is just as important as the new technologies being installed by BSIs. As progress in technology shifts to higher gear, the trend in cyber-attacks, intrusions, and other form of incidents on computer systems shows that it will not only persist but will continue to increase in frequency and spread in magnitude.

Management of IT risks and information security issues becomes a necessity and an important part of BSIs' risk management system. BSIs are therefore required to establish a robust ITRM system covering four (4) key components: 1.) IT governance, 2.) risk identification and assessment, 3.) IT controls implementation, and 4.) risk measurement and monitoring.

1. **IT Governance.** This is an integral part of BSIs' governance framework and consists of the leadership and organizational structures and processes that ensure the alignment of IT strategic plan with BSIs' business strategy, optimization of resources management, IT value delivery, performance measurement and the effective and efficient use of IT to achieve business objectives and effective IT risk management implementation. BSIs must establish an effective IT governance framework covering the following:

a. **Oversight and Organization of IT Functions.** Accountability is a key concern of IT governance and this can be obtained with an organizational structure that has well-defined roles for the responsibility of information, business processes, applications, IT infrastructure, etc.

The Board of Directors is ultimately responsible for understanding the IT risks confronted by a BSI and ensuring that they are properly managed, whereas the Senior Management is accountable for designing and implementing the ITRMS approved by the Board. For Complex BSIs, the Board may delegate to an IT Steering Committee (ITSC) or its equivalent IT oversight function to cohesively monitor IT performance and institute appropriate actions to ensure achievement of desired results. The ITSC, at a minimum, should have as members a non-executive Board director who oversees the institution's IT function, the head of IT group/department, and the highest rank officer who oversees the business user groups. The head of control groups should participate in ITSC meetings in advisory capacity only.

A charter should be ratified by the Board to clearly define the roles and responsibilities of the ITSC. Formal minutes of meeting should be maintained to document its discussions and decisions. The ITSC should regularly provide adequate information to the Board regarding IT performance, status of major IT projects or other significant issues to enable the Board to make well-informed decisions about the BSIs' IT operations.

BSIs should develop an IT strategic plan that is aligned with the institution's business strategy. This should be undertaken to manage and direct all IT resources in line with the business strategy and priorities. IT strategic plan should focus on long term goals covering three to five year horizon and should be sufficiently supplemented by tactical IT plans which specify concise objectives, action plans and tasks that are understood and accepted by both business and IT. The IT strategic plan should be formally documented, endorsed by the Board and communicated to all stakeholders. It should be reviewed and updated regularly for new risks or opportunities to maximize the value of IT to the institution.

BSIs should also create an organization of IT functions that will effectively deliver IT services to business units. For "Complex" BSIs, a full-time IT Head or equivalent rank should be designated to take the lead in key IT initiatives and oversee the effectiveness of the IT organization. In addition to managing the delivery of day-to-day IT services, the IT Head should also oversee the IT budget and maintain responsibility for performance management, IT acquisition oversight, professional development and training. The IT Head should be a member of executive management with direct involvement in key decisions for the BSI and usually reports directly to the President or Chief Executive Officer.

A clear description of roles and responsibilities for individual IT functions should be documented and approved by the Board. Proper segregation of duties within and among the various IT functions should be implemented to reduce the possibility for an individual to compromise a critical process. A mechanism should be in place to ensure that personnel are performing only the functions

relevant to their respective jobs and positions. In the event that an institution finds it difficult to segregate certain IT control responsibilities, it should put in place adequate compensating controls (e.g. peer reviews) to mitigate the associated risks.

b. **IT Policies, Procedures and Standards.** IT controls, policies, and procedures are the foundation of IT governance structure. It helps articulate the rules and procedures for making IT decisions, and helps to set, attain, and monitor IT objectives.

BSIs should adopt and enforce IT-related policies and procedures that are well-defined and frequently communicated to establish and delineate duties and responsibilities of personnel for better coordination, effective and consistent performance of tasks, and quicker training of new employees. Management should ensure that policies, procedures, and systems are current and well-documented. The ITSC should review IT policies, procedures, and standards at least on an annual basis. Any updates and changes should be clearly documented and properly approved. IT policies and procedures should include at least the following areas:

- IT Governance/Management;
- Development and Acquisition;
- IT Operations;
- Communication networks;
- Information security;
- Electronic Banking/Electronic Products and Services; and
- IT Outsourcing / Vendor Management.

For simple BSIs, some of the above areas (i.e. development, electronic banking, etc.) may not be applicable, thus sound judgment should be employed to ensure that the BSI's IT policies and procedures have adequately covered all applicable areas.

c. **IT Audit.** Audit plays a key role in assisting the Board in the discharge of its corporate governance responsibilities by performing an independent assessment of technology risk management process and IT controls.

Auditors provide an assurance that important control mechanisms are in place for detecting deficiencies and managing risks in the implementation of IT. They should be qualified to assess the specific risks that arise from specific uses of IT. BSIs should establish effective audit programs that cover IT risk exposures throughout the organization, risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies and periodic reporting to the Board on the effectiveness of institution's IT risk management, internal controls, and IT governance. Regardless of size and complexity, the IT audit program should cover the following:

- Independence of the IT audit function and its reporting relationship to the Board or its Audit Committee;

- Expertise and size of the audit staff relative to the IT environment;
- Identification of the IT audit universe, risk assessment, scope, and frequency of IT audits;
- Processes in place to ensure timely tracking and resolution of reported weaknesses; and
- Documentation of IT audits, including work papers, audit reports, and follow-up.

In case in-house IT audit expertise is not available, such as for a simple BSI, the IT audit support may be performed by external specialists and auditors of other institutions consistent with existing BSP rules and regulations on outsourcing. (Detailed guidelines/standards on IT Audit are shown in **Appendix 75a**)

d. **Staff Competence and Training.** The rapid development in technology demands appropriate, skilled personnel to remain competent and meet the required level of expertise on an ongoing basis.

BSIs should have an effective IT human resources management plan that meets the requirements for IT and the business lines it supports. Management should allocate sufficient resources to hire and train employees to ensure that they have the expertise necessary to perform their job and achieve organizational goals and objectives.

Management needs to ensure that staffing levels are sufficient to handle present and expected work demands, and to cater reasonably for staff turnover. Appropriate succession and transition strategies for key officers and personnel should be in place to provide for a smooth transition in the event of turnover in vital IT management or operations functions.

e. **Management Information Systems (MIS).** The BSIs' IT organization often provides an important support role for their MIS. Accurate and timely MIS reports are an essential component of prudent and reasonable business decisions. At the most senior levels, MIS provides the data and information to help the Board and management make strategic decisions. At other levels, MIS allows management to monitor the institution's activities and distribute information to other employees, customers, and members of management.

Advances in technology have increased the volume of information available to management and directors for planning and decision-making. However, if technology is not properly managed, the potential for inaccurate reporting and flawed decision making increases. Because report generation systems can rely on manual data entry or extract data from many different financial and transaction systems, management should establish appropriate control procedures to ensure information is correct, relevant, and adequately protected. Since MIS can originate from multiple equipment platforms and systems, the controls should ensure all information systems have sufficient and appropriate controls to maintain the integrity of the information and the processing environment. Sound fundamental principles for MIS review include proper internal controls, operating procedures, safeguards, and audit coverage.

f. **IT Risk Management Function.** Management of risk is a cornerstone of IT Governance. BSIs should have a policy requiring the conduct of identification, measurement, monitoring and controlling of IT risks for each business function/service on a periodic basis. BSIs should define and assign these critical roles to a risk management unit or to a group of persons from different units collectively performing the tasks defined for this function.

The function should have a formal technology risk acknowledgement and acceptance process by the owner of risk to help facilitate the process of reviewing, evaluating and approving any major incidents of non-compliance with IT control policies. The process can be supported by the following:

- a description of risk being considered for acknowledgement by owner of risk and an assessment of the risk that is being accepted;
- identification of mitigating controls;
- formulation of a remedial plan to reduce risk; and
- approval of risk acknowledgement from the owner of the risk and senior management.

ITRM processes should be integrated into the enterprise-wide risk management processes to allow BSIs to make well-informed decisions involving business plans and strategies, risk responses, risk tolerance levels and capital management, among others.

2. **Risk Identification and Assessment.** BSIs should maintain a risk assessment process that drives response selection and controls implementation. An effective IT assessment process begins with the identification of the current and prospective IT risk exposures arising from the institution's IT environment and related processes. The assessments should identify all information assets, any foreseeable internal and external threats to these assets, the likelihood of the threats, and the adequacy of existing controls to mitigate the identified risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels.

   Once management understands the institution's IT environment and analyzes the risk, it should rank the risks and prioritize its response. The probability of occurrence and the magnitude of impact provide the foundation for reducing risk exposures or establishing mitigating controls for safe, sound, and efficient IT operations appropriate to the complexity of the organization. Periodic risk assessment process should be done at the enterprise-wide level and an effective monitoring program for the risk mitigation activities should be manifested through mitigation or corrective action plans, assignment of responsibilities and accountability and management reporting.

3. **IT Controls Implementation.** Controls comprise of policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be mitigated. Management should establish an adequate and effective system of internal controls based on the

degree of exposure and the potential risk of loss arising from the use of IT. Controls for IT environment generally should address the overall integrity of the environment and should include clear and measurable performance goals, the allocation of specific responsibilities for key project implementation, and independent mechanisms that will both measure risks and minimize excessive risk-taking. BSI Management should implement satisfactory control practices that address the following as part of its overall IT risk mitigation strategy: 1) Information security; 2) Project management/development and acquisition and change management; 3) IT operations; 4) IT outsourcing/Vendor management; and 5) Electronic banking, Electronic payments, Electronic money and other Electronic products and services.

a. **Information security.** Information is a vital asset that must be managed to support BSI management in making decisions. BSIs should have a comprehensive information security program, approved by the Board, to maintain the confidentiality, integrity, and availability of computer systems for reliable and timely information. Unauthorized access, destruction, or disclosure of confidential information can adversely affect earnings and capital. The program should monitor information security function throughout the organization's business processes and establish clear accountability for carrying out security responsibilities.

   The Board or Senior Management should appoint an independent information security officer (ISO) who will be responsible and accountable for the organization-wide IS program. The duly appointed ISO should have sufficient knowledge, background, and training, as well as organizational position, to enable him to perform assigned tasks. To ensure appropriate segregation of duties, the ISO should report directly to the Board or senior management and have sufficient independence to perform his mandate. The ISO should perform the tasks of a risk manager and not a production resource assigned to the IT department. In the case of simple BSIs, hiring a personnel to specifically perform the function of an ISO may not be necessary. The ISO function may be assigned to an existing independent officer who meets the requirements mentioned in this subsection. (Detailed guidelines/standards on Information Security are shown in **Appendix 75b**)

b. **Project Management/Development and Acquisition and Change Management.** BSIs should establish a framework for management of IT-related projects. The framework should clearly specify the appropriate project management methodology that will govern the process of developing, implementing and maintaining major IT systems. The methodology, on the other hand, should cover allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, checkpoints, key dependencies, quality assurance, risk assessment and approvals, among others. In the acquisition and/or development of IT solutions, BSIs should ensure that business and regulatory requirements are satisfied. (Detailed guidelines/standards on Project Management/Development and Acquisition and Change Management are shown in **Appendix 75c**)

c. **IT Operations.** IT has become an integral part of the day-to-day business operation, automating and providing support to nearly all of the business processes and functions within the institution. Therefore, the IT systems should be reliable, secure and available when needed which translates to high levels of service and dependency on IT to operate.

One of the primary responsibilities of IT operations management is to ensure the institution's current and planned infrastructure is sufficient to accomplish its strategic plans. BSI management should ensure that IT operates in a safe, sound, and efficient manner throughout the institution. Given that most IT systems are interconnected and interdependent, failure to adequately supervise any part of the IT environment can heighten potential risks for all elements of IT operations and the performance of the critical business lines of the BSIs. Such scenario necessitates the coordination of IT controls throughout the institution's operating environment. (Detailed guidelines/standards on IT Operations are shown in **Appendix 75d**)

d. **IT Outsourcing/Vendor Management Program.** IT outsourcing refers to any contractual agreement between a BSI and a service provider or vendor for the latter to create, maintain, or reengineer the institution's IT architecture, systems and related processes on a continuing basis. A BSI may outsource IT systems and processes except those functions expressly prohibited by existing regulations. The decision to outsource should fit into the institution's overall strategic plan and corporate objectives and said arrangement should comply with the provisions of existing BSP rules and regulations on Outsourcing. Although the technology needed to support business objectives is often a critical factor in deciding to outsource, managing such relationships should be viewed as an enterprise-wide corporate management issue, rather than a mere IT issue.

While IT outsourcing transfers operational responsibility to the service provider, the BSIs retain ultimate responsibility for the outsourced activity. Moreover, the risks associated with the outsourced activity may be realized in a different manner than if the functions were inside the institution resulting in the need for controls designed to monitor such risks. BSI management should implement an effective outsourcing oversight program that provides the framework for management to understand, monitor, measure, and control the risks associated with outsourcing. BSIs outsourcing IT services should have a comprehensive outsourcing risk management process which provide guidance on the following areas: 1) risk assessment; 2) selection of service providers; 3) contract review; and 4) monitoring of service providers. Detailed guidelines/standards on IT Outsourcing/Vendor Management are shown in **Appendix 75e**. Guidelines on the adoption of outsourced cloud computing model are also included therein.

e. **Electronic Products and Services.** The evolution in technology revolutionized the way banking and financial products and services are delivered. Physical barriers were brought down enabling clients to access their accounts, make transactions or gather information on financial products and services anywhere they are, at any time of the day and at their own convenience. As development in technology continues to accelerate, innovative electronic products and services

are foreseen to bring more accessibility and efficiency. However, BSIs may be confronted with challenges relating to capacity, availability and reliability of the electronic services. Likewise, fraudulent activities via electronic channels are also rising in number.

BSIs should protect customers from fraudulent schemes done electronically. Otherwise, consumer confidence to use electronic channels as safe and reliable method of making transactions will be eroded. To mitigate the impact of cyber fraud, BSIs should adopt aggressive security posture such as the following:

- The entire ATM system shall be upgraded/converted to allow adoption of end-to-end Triple DES (3DES) encryption standards by 01 January 2015. The 3DES encryption standards shall cover the whole ATM network which consists of the host processors, switches, host security module (HSM), automated teller machines (ATMs), point-of-sale (POS) terminals and all communication links connected to the network;
- ATMs to be installed after date of issuance of this Circular should be 3DES compliant; and
- ATMs, POS terminals and payment cards are also vulnerable to skimming attacks due to the lack of deployment of globally recognized EMV enabled technology by BSIs. Magnetic stripe only ATMs, POS Terminals and cards are largely defenseless against modern fraud techniques. Therefore, all concerned BSIs should shift from magnetic stripe technology to EMV chip-enabled cards, POS Terminals and ATMs. The entire payment card network should be migrated to EMV by 01 January 2017. This requirement shall cover both issuing and acquiring programs of concerned BSIs. A written and Board-approved EMV migration plan should be submitted to BSP within six (6) months from date of this Circular. Likewise, the detailed guidelines covering subject EMV requirement shall be issued separately.

Detailed guidelines/standards on Electronic Products and Services are shown in **Appendix 75f.**

4. **Risk Measurement and Monitoring.** BSI Management should monitor IT risks and the effectiveness of established controls through periodic measurement of IT activities based on internally established standards and industry benchmarks to assess the effectiveness and efficiency of existing operations. Timely, accurate, and complete risk monitoring and assessment reports should be submitted to management to provide assurance that established controls are functioning effectively, resources are operating properly and used efficiently and IT operations are performing within established parameters. Any deviation noted in the process should be evaluated and management should initiate remedial action to address underlying causes. The scope and frequency of these performance measurement activities will depend on the complexity of the BSI's IT risk profile and should cover, among others, the following:

   a. **Performance vis-à-vis Approved IT Strategic Plan.** As part of both planning and monitoring mechanisms, BSI management should periodically assess its uses of IT as part of overall business planning. Such an enterprise-wide and ongoing

approach helps to ensure that all major IT projects are consistent with the BSI's overall strategic goals. Periodic monitoring of IT performance against established plans shall confirm whether IT strategic plans remain in alignment with the business strategy and the IT performance supports the planned strategy.

b. **Performance Benchmarks/Service Levels.** BSIs should establish performance benchmarks or standards for IT functions and monitor them on a regular basis. Such monitoring can identify potential problem areas and provide assurance that IT functions are meeting the objectives. Areas to consider include system and network availability, data center availability, system reruns, out of balance conditions, response time, error rates, data entry volumes, special requests, and problem reports.

   Management should properly define services and service level agreements (SLA) that must be monitored and measured in terms understandable to the business units. SLA with business units and IT department should be established to provide a baseline to measure IT performance.

c. **Quality Assurance/Quality Control.** BSI should establish quality assurance (QA) and quality control (QC) procedures for all significant activities, both internal and external, to ensure that IT is delivering value to business in a cost effective manner and promotes continuous improvement through ongoing monitoring. QA activities ensure that product conforms to specification and is fit for use while QC procedures identify weaknesses in work products and to avoid the resource drain and expense of redoing a task. The personnel performing QA and QC reviews should be independent of the product/process being reviewed and use quantifiable indicators to ensure objective assessment of the effectiveness of IT activities in delivering IT capabilities and services.

d. **Policy compliance.** BSIs should develop, implement, and monitor processes to measure IT compliance with their established policies and standards as well as regulatory requirements. In addition to the traditional reliance on internal and third party audit functions, BSIs should perform self-assessments on a periodic basis to gauge performance which often lead to early identification of emerging or changing risks requiring policy changes and updates.

e. **External Assessment Program.** Complex BSIs may also seek regular assurance that IT assets are appropriately secured and that their IT security risk management framework is effective. This may be executed through a formal external assessment program that facilitates a systematic assessment of the IT security risk and control environment over time.

§X176.8 ***Reports.*** To enable the BSP to regularly monitor IT risk profile and electronic products, services, delivery channels, processes and other relevant information regarding the use of technology, BSIs are required to submit the following:

1. Annual IT Profile, electronically to the BSP Supervisory Data Center (SDC) within 25 days from the end of reference year (Guidelines to be observed in the preparation and submission of this report was issued under BSP Memorandum to All Banks No. M-2012-011 dated 17 February 2012);

2. Report on breach in information security, especially incidents involving the use of electronic channels, pursuant to the provisions of items "a" or "b" of Subsection X192.4 of the MORB following the guidelines provided in item "d" of the same Subsection. Depending on the nature and seriousness of the incident, BSP may require the BSI to provide further information or updates on the reported incident until the matter is finally resolved; and

3. Notification letter to the Core Information Technology Specialist Group (CITSG) of the BSP of disruption of IT services/operations that resulted to the activation of disaster recovery and business continuity plan immediately upon activation of the plan.

§X176.9 ***Sanctions and Penalties.*** BSIs should make available IT policies and procedures on the foregoing and other related documents during the on-site examination as well as provide a copy thereof when written request was made to determine their compliance with this Circular.

Any violation of the provisions of this Section, its appendices and annexes, shall be subject to the monetary and non-monetary sanctions provided under Section 37 of R.A. No. 7653. Enforcement actions shall be imposed on the basis of the overall assessment of BSIs' ITRMS. Whenever a BSI's ITRMS is rated "1" pursuant Subsection X176.4, the following additional sanctions may be imposed:

1. Suspension/revocation of authority to provide electronic products and services; and
2. Prohibition against offering/provision of new electronic products and services.

Section 2. Repealing Clause. The provisions of Section X176 of the MORB are hereby repealed, amended and/or modified and are also made applicable to non-bank financial institutions under the supervision of Bangko Sentral ng Pilipinas and incorporated as Sections 4176Q, 4196N, 4196S and 4193P of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

The guidelines on consumer protection for electronic banking under Section X705 and Appendices 70a – 70d of the Manual of Regulations for Banks (MORB) are hereby amended and transferred to the IT Risk Management Standards and Guidelines under Subsection X176.7 (3)(e) and Appendix 75f of this Circular.

Section 3. Effectivity. This Circular shall take effect fifteen (15) days following its publication in the official gazette or in any newspaper of general circulation in the Philippines.

FOR THE MONETARY BOARD:

NESTOR A. ESPENILLIA, JR.
Officer-In-Charge

22 August 2013

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: IT Audit

1. INTRODUCTION

1.1. BSIs must plan, manage and monitor rapidly changing technologies to enable them to deliver and support new products, services, and delivery channels. The rate of these changes and the increasing reliance on IT make the inclusion of IT audit coverage essential to an effective overall audit program. The audit program should address IT risk exposures throughout the organization, including the areas of IT management and strategic planning, IT operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic products and services, systems development and acquisition, and business continuity planning. IT audit should also focus on how management determines the risk exposure from its operations and controls or mitigates identified risks.

1.2. A well-planned, properly structured audit program[1] is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT-related risks at BSIs of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies and inform the Board of Directors of the effectiveness of risk management practices. An effective IT audit function may also allow regulators to place substantial reliance on and reduce the time spent reviewing areas of the BSIs during examinations. Ideally, the audit program should consist of a full-time, continuous program of internal audit which may be further supported by a well-planned external audit program.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The BSI's Board or its Audit Committee has the overall responsibility for establishing and maintaining an independent, competent and effective IT audit function commensurate with the complexity of its IT risk profile. In order to properly oversee the IT audit function, the Board or its Audit Committee should:

- Assign responsibility for IT audit function to an internal audit department or individual with sufficient audit expertise, knowledge base and skill level;
- Ensure that IT audit maintains its professional and organizational independence[2]; and
- Approve and review an audit program that would guide IT audit engagements.

Senior management is responsible for supporting IT audit by providing sufficient resources, establishing programs defining and requiring compliance with IT planning practices, operating policies and internal controls. Likewise, senior management

[1] **Audit program** encompasses audit policies, procedures, and strategies that govern the audit function, including IT audit.

[2] **Independence** means self-governance, freedom from conflict of interest and undue influence. The IT auditor should be free to make his or her own decisions, not influenced by the organization being audited, or by its managers and employees.

should not, in any manner, diminish or interfere with the candor of the audit findings and recommendations.

2.2. **Audit Management and Audit Staff.** The internal audit manager is responsible for implementing the Board-approved audit directives. The manager oversees the audit function and provides leadership and direction in communicating and monitoring audit policies, practices, programs, and processes. He should establish clear lines of authority and reporting responsibility for all levels of audit personnel and activities. The internal audit manager should also ensure that members of the audit staff possess the necessary independence, experience, education, training, and skills to properly conduct assigned activities. This can be undertaken by providing auditors with an effective program of continuing education and development. As the information systems of a BSI become more sophisticated or as more complex technologies evolve, the auditor may need additional training.

The primary role of the internal IT audit staff, on the other hand, is to assess independently and objectively the controls, reliability, and integrity of the BSI's IT environment. Internal auditors should evaluate IT plans, strategies, policies, and procedures to ensure adequate management oversight. They should assess the day-to-day IT controls to ensure that transactions are recorded and processed in compliance with acceptable accounting methods and standards and are in compliance with policies set forth by the Board and senior management. Auditors also perform operational audits, including system development audits, to ensure that internal controls are in place, policies and procedures are effective, and employees operate in compliance with approved policies. Auditors should identify weaknesses, provide meaningful recommendations and review management's plans for addressing those weaknesses, monitor their resolution, and report to the Board material weaknesses, as necessary.

2.3. **Operating Management.** Operating management should formally and effectively respond to IT audit or examination findings and recommendations. The audit procedures should clearly identify the methods for following up on noted audit or control exceptions or weaknesses. Operating management is responsible for correcting the root causes of the audit or control exceptions, not just treating the exceptions themselves. Response times for correcting noted deficiencies should be reasonable and may vary depending on the complexity of the corrective action and the risk of inaction.

3. INDEPENDENCE OF THE IT AUDIT FUNCTION

3.1. The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Hence, the placement of the internal audit function in relation to the BSI's management structure should be carefully assessed. The degree of auditors' independence, objectivity and impartiality entails the following key elements:

- Direct reporting of audit results to the Board or its Audit Committee;
- Full authority vested by the Board to the IT Audit Department/IT auditor to access all records and staff necessary to conduct the audit and require management to address significant findings in a timely manner. Said authority must be clearly

specified in an Internal Audit Charter or Audit Program duly approved by the Board or Audit Committee;

- Non-involvement of IT audit personnel in management/operational activities that may compromise or appear to compromise their independence; and
- The Board or Audit Committee should decide on audit personnel performance evaluation and compensation matters.

4. INTERNAL IT AUDIT PROGRAM

4.1. A formal audit program or manual consisting of policies and procedures governing the IT audit function should be adopted commensurate with the BSI's size, complexity, scope of activities and risk profile. The audit program should, at a minimum, encompass the following components:

- A mission statement or audit charter[3] outlining the purpose, objectives, organization, authorities, and responsibilities of the internal auditor, audit staff, audit management, and the audit committee;
- A risk assessment process to describe and analyze the risks inherent in a given line of business and drive the scope and frequency of audits. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes;
- An annual audit plan detailing IT audit's budgeting and planning processes to include audit goals, schedules, staffing needs and reporting;
- An audit cycle that identifies the frequency of audits which should be based on a sound risk assessment process;
- Well-planned and properly structured audit work programs[4] that set out the required scope and resources, including the selection of audit procedures, extent of testing and the basis for conclusions for each audit area;
- Audit report preparation standards that require the use of an approved audit rating system;
- Requirements for audit work paper documentation to ensure clear support for all audit findings and work performed, including work paper retention policies;
- Follow-up processes that require internal auditors to determine the disposition of management actions to correct significant deficiencies;
- Policies on outsourcing of some or all of IT audit function, including technical/highly specialized reviews, to external third parties; and
- Professional development programs for audit staff/personnel to maintain the necessary technical expertise.

Additionally, the BSI should consider conducting its internal audit activities in accordance with professional standards, such as the *Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors (IIA), and those issued by the Standards Board of the Information Systems Audit and Control Association (ISACA), whenever possible.

---

[3] **Audit charter** is a document approved by the Board of Directors that defines the IT audit function's responsibility, authority and accountability.

[4] **Work program** is a series of specific, detailed steps to achieve an audit objective.

5. IT AUDIT PHASES

5.1. **Audit Planning.** The BSI should develop an overall audit plan[5] for all the audit assignments/engagements covering at least 12 months to ensure adequate coverage of IT risks. The plan should be defined by combining the results of the risk assessments and the resources required to yield the timing and frequency of planned internal audits. The audit plan must be realistic and should cover a time budget for other assignments and activities such as specific examination, consulting/advisory services, training and provision for audit personnel leave of absences.

The audit plan must be formally approved and regularly reviewed by the Board or Audit Committee. The internal auditors should report the status of the planned versus actual audits and any revisions to the annual audit plan on a periodic basis.

For each audit assignment, an audit work program detailing the objectives, scope, nature and extent of audit procedures and outline of audit work should be prepared. This is to ensure that appropriate attention is devoted to important areas of the audit, potential problems are identified and resolved on a timely basis, and the audit engagement is properly organized and managed to be performed in an effective and efficient manner.

5.2. **Risk Assessment.** The use of an appropriate risk assessment technique or approach is critical in developing the overall IT audit plan and in planning specific audits. An effective risk assessment methodology should be defined to provide the Board or its Audit Committee with objective information in determining audit priorities for the effective allocation of IT audit resources. The risk assessment for IT audit planning should:

- Identify the BSI's data, application[6] and operating systems[7], technology, facilities, and personnel;
- Identify the business activities and processes within each of those categories;
- Include profiles of significant business units, departments, and product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the BSI; and
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products.

The results of the risk assessments, in support of the audit plan, must be presented to the Board or Audit Committee for review and approval. A process must be in place to ensure regular monitoring of the results of the risk assessment and updating it at least annually for all significant business units, departments, and products or systems.

---

[5] **Audit plan** is a description and schedule of audits to be performed in a certain period of time (ordinarily a year). It includes the areas to be audited, the type of work planned, the high-level objectives and scope of the work and includes other items such as budget, resource allocation, schedule dates, and type of report issued.

[6] **Application system** is an integrated set of computer programs designed to serve a well-defined function and having specific input, processing, and output activities (e.g., CASA, general ledger, loans and treasury systems).

[7] **Operating system** is the program that manages all the basic functions and programs in a computer.

A risk scoring model or system may be adopted to provide a sound basis for the risk assessment. Among the major risk factors that may be used in scoring systems include the following: a) Adequacy of internal controls; b) Nature of transactions and operating environment; c) Age of the system or application; d) Physical and logical security of information, equipment, and premises; e) Adequacy of operating management oversight and monitoring; f) Previous regulatory examination and audit results and management's responsiveness in addressing issues; g) Human resources, including the experience of management and staff, turnover, technical competence, management's succession plan, and the degree of delegation; and h) Senior management oversight.

Written guidelines on the use of risk assessment tools and risk factors should be approved and reviewed by the Board or its Audit Committee. IT auditors should use the guidelines to grade or assess major risk areas and to define the range of scores or assessments (e.g. groupings such as high, medium or low risk or numeric risk ratings). At a minimum, the written assessment guidelines should specify the following elements: a) Maximum length for audit cycles based on the risk scores; b) Timing of risk assessments for each department or activity; c) Documentation requirements to support scoring decisions; and d) Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden.

5.3. **Performance of Audit Work.** Depending on the complexity of IT risk profile, IT auditors may perform all or a combination of any of the following IT audit procedures:

- ***IT General Controls Review*** - This entails the review of the adequacy of general controls[8] in place to ensure proper management and monitoring of IT risks/environment and the effective functioning of the BSI's IT systems and infrastructure. The following areas should be covered, among others: a) IT management and strategic planning; b) IT operations; c) Client/server architecture; d) Local and wide-area networks; e) Telecommunications; and f) Physical and information security.

  IT general controls review may be carried out through the audit of each IT unit or department in the institution (e.g. IT Operations, Network and Communications, etc.).

- ***Application Systems Review*** - The purpose of this review is to identify, document, test and evaluate the application controls[9] that are implemented to ensure the

[8] **General controls** are controls, other than application controls, that relate to the environment within which application systems are developed, maintained, and operated, and that are therefore applicable to all the applications at an institution. Like application controls, general controls may be either manual or automated. Examples of general controls include the development and implementation of an IT strategy and an IT security policy, the organization of IT staff to separate conflicting duties and planning for disaster prevention and recovery.

[9] **Application controls** are controls related to transactions and data within application systems. Application controls ensure the completeness and accuracy of the records and the validity of the entries made resulting from both programmed processing and manual data entry. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.

confidentiality, integrity and accuracy of the system processing and the related data. The application-level risks to the system and data addressed by this review are the following, among others: a) System availability risks relating to the lack of system operational capability; b) System security risks relating to unauthorized access to systems and/or data; c) System integrity risks relating to incomplete, inaccurate, untimely or unauthorized processing of data; d) System maintainability risks relating to inability to update the system when required in a manner that continues to provide for system availability, security and integrity; and e) Data risks relating to its completeness, integrity, confidentiality, privacy and accuracy.

- ***Technical Reviews*** - BSIs with complex IT risk profile such as those providing electronic products and services and web-enabled facilities, also require IT auditors to perform highly technical/specialized reviews such as the conduct of periodic internal vulnerability assessment and penetration testing, computer forensics and review of emerging technologies, e.g. cloud computing, virtualization, mobile computing.

IT auditors frequently use computer-assisted audit techniques (CAATs) to improve audit coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. CAATs include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert systems. These tools and techniques can also be used effectively to check data integrity by testing the logical processing of data "through" the system, rather than by relying only on validations of input and output controls.

Audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings, source and object program modules, and all changes to such programs, should be strictly controlled. Computer programs intended for audit use should be carefully documented to define their purpose and to ensure their continued usefulness and reliability.

All audit procedures forming part of the assignment should be documented in working papers. These must reflect the examinations that have been made and emphasize the evaluations formulated in the report. The working papers must be drawn up according to a well-determined method. Such method must provide sufficient information to verify whether the assignment was duly performed and to enable others to check the manner in which it was performed.

5.4. **Reporting.** A written audit report of each assignment is to be issued to the auditee and Audit Committee within a reasonable timeline. The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed. It should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IT auditor has with respect to the audit. The IT audit should discuss the draft report contents with management in the subject area prior to finalization and release of the final report. This should be signed, dated and distributed according to the terms of the audit charter/audit program or engagement letter.

5.5. **Post-closing/Monitoring Activities.** Senior management should ensure that the internal audit department's concerns are appropriately addressed. Therefore, they should approve a procedure established by the internal audit department to ensure the consideration and, if appropriate, timely implementation of audit recommendations.

The IT audit department should monitor the implementation of management's corrective actions for proper disposition of its findings/recommendation. The status of the recommendations is communicated at least on a quarterly basis to the Board or Audit Committee.

6. OTHER IT AUDIT ACTIVITIES/PARTICIPATION

6.1. **Development, Acquisition, Conversions and Testing.** The BSI's Board-approved audit policy should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. This includes describing the monitoring, reporting, and escalation processes (when internal controls are found to be insufficient or when testing is found to be inadequate). For acquisitions with significant IT impacts, participation of IT audit may be necessary early in the due diligence stage.

It is necessary that audit's participation in the development process be independent and objective. Auditors can determine and should recommend appropriate controls to project management. However, such recommendations do not necessarily "pre-approve" the controls, but instead guide the developers in considering appropriate control standards and structures throughout their project.

6.2. **Review of Technology Service Providers (TSP).** The BSI should effectively manage its relationships with key TSPs through review and assessment of adequacy of IT controls employed by such TSPs. When circumstances warrant, the BSI's internal audit function may be utilized to directly audit TSP's operations and controls. In some instances, the services of external auditors may be employed. A BSI using external audit to complement its own coverage should ensure that the independent auditor is qualified to perform the review, that the scope satisfies its own audit objectives and that any significant reported deficiencies are corrected.

7. OUTSOURCING OF IT AUDIT FUNCTIONS

7.1. The Board and senior management of a BSI that outsources its internal IT audit function should ensure that the structure, scope and management of the outsourcing arrangement provides for an adequate evaluation of the system of internal controls. Management should ensure that there are no conflicts of interest and that the use of these services does not compromise independence.

7.2. When negotiating the outsourcing arrangement with a service provider, the BSI should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. To clearly define the BSI's duties and those of

the audit provider, it should have a written contract, often referred to as an engagement letter[10].

8. COMPLIANCE WITH EXISTING BSP RULES AND REGULATIONS

8.1. The provisions of the IT audit guidelines prescribe in detail the essentials and elements of an effective IT audit which complement and are consistent with Subsection *X185.9 Independence of the Internal Auditor* of the Manual of Regulations for Banks (MORB). Likewise, the IT audit-related tasks of the Audit Committee are in addition to the tasks prescribed under *X141.3 Powers/responsibilities and duties of directors, item 9.a.* of the MORB, as amended by Circular No. 749, Series of 2012.

[10] In general, the contract between the institution and the audit provider may or may not be the same as the engagement letter.

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: Information Security

1. INTRODUCTION

1.1. Information is one of the most important assets of all BSIs. Timely and reliable information is necessary to process their transactions and support critical decisions. Protection of information assets is also necessary to establish and maintain trust between the BSIs and their customers, maintain compliance with laws and regulations and protect reputation. Likewise, effective management of information risks and exposures—as well as opportunities—can directly affect the BSIs' profitability and overall value.

1.2. Information security (IS) has become a critical business function and an essential component of governance and management affecting all aspects of the business environment. Effective IS controls are necessary to ensure the confidentiality, integrity and availability of IT resources and their associated data. These assets should be adequately protected from unauthorized access, deliberate misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure. To achieve these objectives, BSIs should establish an IS program to manage the risks identified through their assessment, commensurate with the sensitivity of the information and the complexity of their IT risk profile. Management may consider a variety of policies, procedures, and technical controls and adopt measures that appropriately address identified risks.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The Board, or an appropriate Board committee, is responsible for overseeing the development, implementation, and maintenance of the BSI's IS program, and making senior management accountable for its actions. The Board should approve written IS policies and receive periodic report on the effectiveness of the IS program. The IS policy should be communicated to all employees and relevant external parties and be reviewed at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The policy should include a formal disciplinary process and the corresponding actions for those who have committed security violations.

Senior management should appoint an information security officer (ISO) who will be responsible and accountable for the organization-wide IS program. The duly appointed ISO should have sufficient knowledge, background, and training, as well as organizational position, to enable him to perform assigned tasks. To ensure appropriate segregation of duties, the ISO should report directly to the Board or to senior management and have sufficient independence to perform his mandate. The ISO should perform the tasks of a risk manager and not a production resource assigned to the IT department. In the case of BSIs with simple IT risk profile, The ISO function may be assigned to an existing independent officer who meets the above qualifications.

3. INFORMATION SECURITY STANDARDS

3.1. **IS Risk Assessment.** The BSI should conduct periodic security risk assessment to identify and understand risks on confidentiality, integrity and availability of information and IT systems based on a current and detailed knowledge of the BSI's operating and business environments. The risk assessment should include an identification of information and IT resources to be protected and their potential threats and vulnerabilities. An effective risk assessment process involves three phases, namely: information gathering, analysis, and prioritizing responses. Vendor concerns add additional elements to the process.

Once the risks associated with threats and vulnerabilities have been assessed, probabilities assigned, and risks rated, the BSI should segregate the risks into those the BSI is willing to accept and those that should be mitigated. Once the BSI identifies the risks to mitigate, it can begin to develop its risk mitigation strategy which should be an integral component of the IS program.

3.2. **Security Controls Implementation**

3.2.1. **Asset Classification and Control.** The BSI should maintain an inventory of all information assets and identify the information owner who shall be responsible in ensuring confidentiality, integrity and protection of these assets. Management should implement an information classification strategy in accordance with the degree of sensitivity and criticality of information assets to the BSI. To ensure consistent protection of information and other critical data throughout the system, the BSI should develop guidelines and definitions for each classification and define an appropriate set of controls and procedures for information protection in accordance with the classification scheme.

Protection of information confidentiality should be in place regardless of the media[11] (including paper and electronic media) in which the information is maintained. The BSI should ensure that all media are adequately protected, and establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.

3.2.2. **Physical and Environmental Protection.** Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access. Critical information processing facilities should be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas should be restricted to authorized personnel only and the access rights should be reviewed and updated regularly. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities.

The BSI should fully consider the environmental threats (e.g. proximity to dangerous factories) when selecting the locations of its data centers.

[11] **Media** are physical objects that store data, such as paper, hard disk drives and compact disks.

Moreover, physical and environmental controls should be implemented to monitor environmental conditions which could adversely affect the operation of information processing facilities (e.g. fire, explosives, smoke, temperature, water and dust). Equipment and facilities should be protected from power failures and electrical supply interference by, for example, installing uninterruptible power supply (UPS) and a backup generator.

3.2.3. **Security Administration and Monitoring.** A security administration function and a set of formal procedures should be established for administering the allocation of access rights to system resources[12] and application systems, and monitoring the use of system resources to detect any unusual or unauthorized activities.

Proper segregation of duties within the security administration function or other compensating controls (e.g. peer reviews) should be in place to mitigate the risk of unauthorized activities being performed by the security administration function. In those cases where complete segregation of duties is impractical, management should use mitigating controls, such as ensuring a knowledgeable third-party conducts appropriate independent reviews of security administration activities. In smaller institutions, a manager or senior officer who is not involved in the security administration function may conduct this independent review.

Management should employ the "least privilege" principle throughout IT operations. The principle provides that individuals should only have privileges on systems and access to functions that are required to perform their job function and assigned tasks. Individuals with systems and security administrator roles and privileges should have minimal transactional authority. Independent employees should monitor the system and security administrator activity logs for unauthorized activity. Management at smaller institutions should establish compensating controls in these circumstances.

3.2.4. **Authentication[13] and Access Control.** Access rights and system privileges must be based on job responsibility and the necessity to have them to fulfill one's duties. No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization[14] should be allowed to access confidential information and use system resources solely for legitimate purposes.

The BSI should have an effective process to manage user authentication and access control. Appropriate user authentication mechanism commensurate with the classification of information to be accessed should be selected. The

[12] **System resources** are capabilities that can be accessed by a user or program either on the user's machine or across the network. Capabilities can be services, such as file or print services, or devices, such as routers.

[13] **Authentication** involves verification of identity by a system based on the presentation of unique credentials to that system

[14] **Authorization** is the process of giving access to parts of a system, typically based on the business needs and the role of the individual within the system

grant, modification and removal of user access rights should be approved by the information owner prior to implementation. A user access re-certification process should be conducted periodically to ensure that user access rights remain appropriate and obsolete user accounts have been removed from the systems.

Users who can access internal systems should be required to sign an acceptable-use policy (AUP) before using a system. An AUP is a key control for user awareness and administrative policing of system activities which details the permitted system uses and user activities and the consequences of non-compliance.

The BSI should implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis. Stronger authentication methods should be adopted for transactions/activities of higher risk (e.g. payment transactions, financial messages and mobile computing).

Default user accounts to new software and hardware should either be disabled, or the authentication to the account should be changed. Additionally, access to these default accounts should be monitored more closely than other accounts. In the same manner, authorization for privileged access should be tightly controlled as it gives the user the ability to override system or application controls. Extra care should be exercised when controlling the use of and access to privileged and emergency IDs. The necessary control procedures include:

- Granting of authorities that are strictly necessary to privileged and emergency IDs;
- Formal approval by appropriate personnel prior to being released for usage;
- Monitoring of activities performed by privileged and emergency IDs (e.g. peer reviews of activity logs);
- Proper safeguard of privileged and emergency IDs and passwords (e.g. kept in a sealed envelope and locked up inside the data center); and
- Change of privileged and emergency IDs' passwords immediately upon return by the requesters.

3.2.5. **System Security.** The following control procedures and baseline security requirements should be developed to safeguard operating systems, system software and databases[15], among others:

- Clear definition of a set of access privilege for different groups of users and access to data and programs is controlled by appropriate methods of identification and authentication of users together with proper authorization;
- Secure configuration of operating systems, system software, databases and servers to meet the intended uses with all unnecessary services and

[15] **Database** is an organized collection of information stored on one or more electronic files.

programs disabled or removed. Use of security tools should be considered to strengthen the security of critical systems and servers;
- Periodic checking of the integrity of static data (e.g. system parameters) to detect unauthorized changes;
- Clear establishment of responsibilities to ensure that the necessary patches and security updates developed from time to time by relevant vendors are identified, assessed, tested and applied to the systems in a timely manner;
- Adequate documentation of all configurations and settings of operating systems, system software, databases and servers; and
- Adequate logging and monitoring of system and user activities to detect irregularities and logs are securely protected from manipulation.

3.2.6. **Network Security.** Networks provide system access and connectivity between business units, affiliates, service providers, business partners, customers, and the public. This increased connectivity requires additional controls to segregate and restrict access between various groups and information users. The BSI must evaluate and implement appropriate controls relative to the complexity of its network. An effective approach to adequately secure system and data within the network involves the following, among others:

- Grouping of network servers, applications, data, and users into security domains (e.g., untrusted external networks, external service providers, or various internal user systems);
- Establishment of appropriate access requirements within and between each security domain;
- Implementation of appropriate technological controls to meet access requirements consistently; and
- Monitoring of cross-domain access for security policy violations and anomalous activity.

The BSI should consider the following factors in determining the network security controls appropriate to the institution and each of the security domain, among others:

- Criticality of the application and the user group within the domain;
- Access points to the domain through various communication channels;
- Network protocols and ports used by the applications and network equipment deployed within the domain;
- Performance requirement or benchmark;
- Nature of domain (i.e. production or testing, internal or external);
- Connectivity between/among various domains; and
- Trustworthiness of the domain.

3.2.7. **Remote Access.** Controls over remote access are required to manage risk brought about by external connections to the BSI's network and computing resources. In protecting information, the BSI should establish control procedures covering:

- Approval process on user requests;

- Authentication controls for remote access to networks, host data and/or systems;
- Protection (e.g. against theft and malicious software) of equipment and devices;
- Logging and monitoring all remote access communications; and
- Provision of more stringent security controls (i.e. data encryption, two-factor authentication process).

3.2.8. **Encryption.** The BSI should adopt industry-accepted cryptographic solutions and implement sound key management practices to safeguard the associated cryptographic keys. Sound practices of key management generally include the following, among others:

- Provision of a secure control environment for generation, distribution, storage, entry, use and archiving of cryptographic keys to safeguard against modification and unauthorized disclosure. In particular, the use of tamper-resistant storage is recommended to prevent the disclosure of the cryptographic keys; and
- Adequate off-site back-up and contingency arrangements for cryptographic keys which are subject to the same security controls as the production cryptographic keys.

3.2.9. **Malicious Code[16] Prevention.** The BSI should provide protection against the risk of malicious code by implementing appropriate controls at the host and network level to prevent and detect malicious code, as well as engage in appropriate user education. Procedures and responsibilities should be established to detect, prevent, and recover from attacks. The BSI should put in place adequate controls, such as:

- Prohibiting the download and use of unauthorized files and software, and access to doubtful web sites;
- Installation and timely update of anti-virus software[17] provided by reputable vendors; and
- Disallowing the download of executable files and mobile codes, especially those with known vulnerabilities (e.g. through the use of corporate firewalls[18] and proper configuration of the browser software); and
- Prompt and regular virus scanning of all computing devices and mobile users' computers, and procedures for recovering from virus infections.

3.2.10. **Personnel Security.** The BSI should have a process to verify job application information on all new employees. Screening procedures, including verification and background checks, should be developed for recruitment of

[16] **Malicious code** refers to any code in any part of a software or script that is intended to cause undesired effects, security breaches or damage to a system. It describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

[17] **Antivirus software** is a computer program that offers protection from viruses by making additional checks of the integrity of the operating system and electronic files. Also known as virus protection software.

[18] **Firewall** is a hardware and/or software that prevents unauthorized data from entering or leaving a secure network. Firewalls can also be used to isolate or protect a particular segment of a network.

permanent and temporary IT staff, and contractors, particularly for sensitive IT-related jobs or access level.

Management should obtain signed confidentiality, non-disclosure and authorized use agreements before granting new employees and contractors access to IT systems. Such agreements put all parties on notice that the BSI owns its information, expects strict confidentiality, and prohibits information sharing outside legitimate business needs.

All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate IS awareness training and regular updates in organizational policies and procedures relevant to their job function. Security training and awareness promotes a security conscious environment and strengthens compliance with BSI's security policies, standards, and procedures.

3.2.11. **Systems Development, Acquisition and Maintenance.** A framework should be in place describing the tasks and processes for development or acquisition of new systems, assignment and delineation of responsibilities and accountabilities for system deliverables and project milestones. User functional requirements, systems design and technical specifications and service performance expectations should be adequately documented and approved at appropriate management levels.

The BSI's development, acquisition, and audit policies should include guidelines describing the involvement of internal audit and information security personnel in the development or acquisition activities as a means of independently verifying the adequacy of the control and security requirements as they are developed and implemented.

Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling should be clearly specified. The information and/or process owners should conform to the security requirements for each new system or system acquisition, accept tests against the requirements, and approve implementation of systems in the production environment.

The BSI should have an effective process to introduce application and system changes into its respective environments. The process should encompass development, implementation, and testing of changes to both internally developed software and acquired software. Weak procedures can corrupt applications and introduce new security vulnerabilities.

3.2.12. **Insurance.** While insurance coverage is an effective method to transfer risks from the BSI to insurance carriers, the same is not a substitute for an effective IS program. When considering supplemental insurance coverage for security incidents, the BSI should assess the specific threats in light of the impact these incidents will have on its financial, operational, and reputation risk profiles. The BSI should carefully evaluate the extent and availability of

coverage in relation to the specific risks they are seeking to mitigate. In case the BSI contracts for additional coverage, it should ensure that it is aware of and prepared to comply with any required security controls both at inception of the coverage and over the term of the policy.

3.3. Security Process Monitoring and Updating

3.3.1. **Activity Monitoring.** The BSI should gain assurance of the adequacy of its risk mitigation strategy and implementation by monitoring network and host activity to identify policy violations and anomalous behavior. The BSI's security monitoring should, commensurate with the risk, be able to identify control failures before a security incident occurs, detect an intrusion or other security incident in sufficient time to enable an effective and timely response, and support post-event forensics activities.

The analysis and response to activity and condition monitoring is performed differently at BSIs of different IT risk profile. A simple BSI may assign operational personnel to the analysis and response function while a complex BSI may maintain a security response center that receives and analyzes the data flows as activity occurs. Additionally, BSIs, regardless of IT risk profile, may outsource various aspects of the analysis and response function, such as activity monitoring. Outsourcing does not relieve the BSI of the responsibility for ensuring that control failures are identified before a security incident occurs, an intrusion or other security incident is detected in sufficient time to enable an effective and timely response, and post event forensics activities are supported.

3.3.2. **IS Incident Management.** The BSI should establish incident response and reporting procedures to handle IS-related incidents. All employees, contractors and third party users shall be required to note and report any observed or suspected security weaknesses in systems. An effective incident response program includes the following components, among others:

- A mechanism to log, monitor and quantify the nature, criticality and estimated cost of IS incidents.
- Assessment of the nature and scope of the incident and identification of what information has been accessed or misused;
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of information, while preserving records and other evidence;
- Prompt notification to BSP of any confirmed IT-related fraud cases or major security breaches, consistent with existing regulations;
- Notification to appropriate law enforcement authorities in situations involving criminal violations requiring immediate attention; and
- Notification to customers when warranted.

Log files are critical to the successful investigation and prosecution of security incidents and can potentially contain sensitive information. Therefore, the BSI should strictly control and monitor access to log files whether on the host or in a centralized logging facility.

Where a follow-up action against a person or organization after an IS incident involves legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction.

3.3.3. **Ongoing risk assessment.** The BSI should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on the institution or others, and the effectiveness of the existing security controls. It should evaluate the information gathered to determine the extent of any required adjustments to the various components of the IS program. Depending on the nature of changing environment, the BSI needs to reassess the risk and make changes to its security process (e.g. security strategy, controls implementation or security monitoring requirements).

The BSI should adjust its IS program to reflect the results of ongoing risk assessment and the key controls necessary to safeguard customer information and ensure the proper disposal of customer information. It should adjust the program to take into account changes in IT, sensitivity of its customer information, internal or external threats, and the BSI's own changing business arrangements such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

4. ROLES OF IT AUDIT AND SECURITY SPECIALISTS

4.1. Audit and Compliance Reviews. IT auditors are usually charged to assess, on a regular basis, the effectiveness of a BSI's IS security program. To fulfill this task, they must have an understanding of the protection schemes, the security framework and the related issues, including compliance with applicable laws and regulations.

The BSI should engage independent security specialists to assess the strengths and weaknesses of critical applications, systems and networks prior to initial implementation.

For BSIs providing electronic and similar services, annual vulnerability assessment[19] and penetration testing[20] should be performed by an external party to provide early identification of threats and vulnerabilities so that appropriate security measures can immediately be implemented.

[19] **Vulnerability assessment** (also known as vulnerability analysis) is a process that defines, identifies, and classifies the security flaws (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability assessment can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

[20] **Penetration test** is the process of using approved, qualified personnel to conduct real-world attacks against a system so as to identify and correct security weaknesses before they are discovered and exploited by others.

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: Project Management/Development, Acquisition and Change Management

1. INTRODUCTION

1.1. Because technology is constantly evolving, Management of BSIs should periodically assess their uses of IT as part of overall business planning. Such an enterprise-wide and ongoing approach should be formalized in the IT strategic plan to help ensure that all major IT projects are consistent with its overall strategic goals.

1.2. As part of their strategic goals, BSIs may need to constantly introduce new or enhanced products and services, improve systems and processes and implement updates and innovations in IT to secure and manage voluminous information and maintain their competitive position. This necessity may oftentimes result to initiating IT projects[21]; which may be in the form of internal or external development of software applications or systems, acquisition and/or implementation of new or enhanced hardware, software, infrastructure or services with or without the help of third party providers.

1.3. IT projects, when managed improperly, often result in late deliveries, cost overruns, or poor quality applications. Inferior applications can result in underused, unsecure, or unreliable systems. Retrofitting functional, security, or automated-control[22] features into applications is expensive, time consuming, and often results in less effective features. Therefore, BSIs should carefully manage IT-related projects to ensure they meet organizational needs on time and within budget.

2. ROLES AND RESPONSIBILITIES

2.1. The size and complexity of a project dictates the required number and qualifications of project personnel. Duties may overlap in smaller organizations or lower-risk projects; however, all projects should include appropriate segregation of duties or compensating controls.

2.2. **Board of Directors (Board) and Senior Management.** The BSI's Board and senior management should review, approve, and monitor IT projects that may have significant impact on its operations, earnings or capital. They are responsible to ensure that IT projects support business objectives and adequate resources are available to complete these projects. Consequently, they should establish adequate policies and strategies to achieve these and ensure that risks related to IT projects are managed appropriately.

Senior management is expected to have more knowledge and involvement in the day-to-day operations of these IT projects to critically evaluate the design and oversee the related operation and activities. They should ensure that IT projects are coordinated and undertaken in adherence to appropriate policies, standards, and risk management controls. They should periodically inform the Board and/or IT

[21] An **IT project** is a task involving the acquisition, development or maintenance of a technology product.
[22] **Automated controls** are software routines designed into programs to ensure the validity, accuracy, completeness and availability of input, processed and stored data.

Steering Committee of the IT initiatives and the related risks that these may pose to the BSI. They should also review, approve, document and report deviations from established policies and standards.

2.3. **Quality Assurance.** An independent party (e.g. the quality assurance function, the TRM function or the technology audit team), who is not involved in the project development, should conduct a quality assurance review of major IT-related projects, with the assistance of the legal and compliance functions, if necessary. This review is to ensure compliance with the project life cycle[23] methodology, other internal policies, control requirements, regulations and applicable laws.

3. PROJECT MANAGEMENT STANDARDS AND METHODOLOGY

3.1. **Project Management.** The BSI should establish a general framework for management of major technology-related projects. This framework should, among other things, specify the project management methodology to be adopted and applied to these projects. The methodology should cover, at a minimum, allocation of responsibilities, activity breakdown, budgeting of time and resources, milestones, check points, key dependencies, quality assurance, risk assessment and approvals.

A BSI that needs to coordinate multiple IT projects should establish standards for coordinating and managing the projects from an enterprise-wide perspective. The standards should, at a minimum, include guidelines for project prioritization, resource coordination and progress reporting.

3.2. **Project Methodology.** The BSI should adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this should involve phases of project initiation, feasibility study, requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance.

The project life cycle methodology should define clearly the roles and responsibilities for the project team and the deliverables[24] from each phase. It also needs to contain a process to ensure that appropriate security requirements are identified when formulating business requirements, built during program development, tested and implemented.

4. PROJECT PLANNING AND INITIATION

4.1. A formal project committee, to ensure the development of well-structured applications, should be established with clear details of its terms and reference. The committee should at least consist of the following representatives:

- o Senior management, to provide strategic direction and ensure full commitment;
- o User departments, to ensure that the application design meets their requirements;

[23] **Project life cycle** refers to a logical sequence of activities to accomplish a project's goals or objectives.

[24] **Deliverables** are project goals and expectations. They include broadly-defined, project or phase requirements and specifically-defined tasks within project phases.

- Internal audit department, to act as in independent party to ensure adequate controls are diligently applied at all times. However, internal audit participation should only be on an advisory capacity; and
- IT department, to provide technical knowledge and skills.

4.2. A feasibility study should be performed to identify the expected costs and benefits of developing a system, and also to decide either to utilize internal resources or to outsource to a vendor. In case of outsourcing, the responsibility of the senior management does not diminish in ensuring that a well-designed application is developed. The senior management maintains the responsibility for ensuring that minimum controls are in place and are in accordance with the BSI's standards.

4.3. When management proposes a new hardware, software or IT solution and/or changes to existing ones, it should ensure that functional, operational and regulatory requirements are accurately identified and clearly detailed in request for proposals (RFP[25]) or invitations-to-tender (ITT) that it distributes to vendors or third-party service providers (TSP) in the bid solicitation process. Moreover, relevant security requirements should be clearly specified before a new system is developed or acquired. A review should also be conducted to ensure an appropriate balance between security and other objectives (ease-of-use, operational simplicity, ability to upgrade, acceptable cost, etc.) is achieved.

4.4. During the development and acquisition of new systems or other major IT projects, project plans should address issues such as – a) business requirements for resumption and recovery alternatives; b) information on back-up and storage; c) hardware and software requirements at recovery locations; d) BCP and documentation maintenance; e) disaster recovery testing; and f) staffing and facilities. Likewise, during maintenance, where there are changes to the operating environment, business continuity considerations should be included in the change control process and implementation phase.

4.5. Proper planning should be employed to ensure IT projects meet their objectives. Project control systems should be employed to monitor specific target completion dates for each task of systems development against original targets. Periodic reports to senior management such as, project priorities and status, resource allocations, target deviations and budgets, should be in place to measure project effectiveness.

5. SYSTEMS DEVELOPMENT

5.1. Development projects involve the creation of applications, integrated application systems and other critical softwares. Software development projects are completed in-house, through outsourcing, or by a combined approach. To manage this type of projects, the BSI should establish development standards that, at a minimum, address project management, system control, and quality assurance issues. Project management standards should address issues such as project management methodologies, risk management procedures, and project approval authorities.

[25] **RFP** is a document that a BSI sends to a vendor inviting the vendor to submit a bid for hardware, software, services, or any combination of the three. An institution typically issues the RFP in order to assess competing bids.

System control standards should address items such as an application's functional, security, and automated control features. Quality assurance standards should address issues such as the validation of project assumptions, adherence to project standards, and testing of a product's performance.

5.2. Development standards should also include procedures for managing internally developed spreadsheets and database reports. BSIs often rely on the spreadsheets and reports to make important budgeting and asset/liability decisions, but fail to implement adequate testing, documentation, and change-control procedures. Management's reliance on the spreadsheets and reports should dictate the formality of their development procedures, change controls, and backup techniques.

5.3. Programming standards should be designed to address issues such as the selection of programming languages and tools, the layout or format of scripted code, interoperability between systems, and the naming conventions of code routines and program libraries. These will enhance the BSI's ability to decrease coding defects and increase the security, reliability, and maintainability of application programs.

6. SYSTEM ACQUISITION

6.1. Software package acquisition is an alternative to in-house systems development and should be subject to broadly similar controls as the project life cycle. A proper software selection analysis should be conducted to ensure that user and business requirements are met. In particular, the process should involve detailed evaluation of the software package and its supplier (e.g. its financial condition, reputation and technical capabilities). If financial stability is in doubt, alternatives should be developed to reduce the adverse impact from loss of a vendor's service.

6.2. The contract agreement between the BSI and vendor should be legally binding. The BSI should ensure all contract agreements outline all expected service levels and are properly executed to protect its interest. It is also important to ensure that vendor technicians and third-party consultants are subjected to at least, or preferably more stringent policies and controls compared to the in-house staff. In the case where contract personnel are employed, written contracts should also be in effect.

7. CHANGE MANAGEMENT

7.1. Change management is the process of planning, scheduling, applying, distributing and tracking changes to application systems, system software (e.g. operating systems and utilities), hardware, network systems, and other IT facilities and equipment. The change management procedures should be formalized, enforced and adequately documented. Authorization and approval are required for all changes and the personnel responsible for program migration should be identified. For the purpose of accountability, proper sign-off should be adequately implemented where formal acknowledgement is obtained from all related parties.

7.2. An effective change management process helps to ensure the integrity and reliability of the production environment. To ensure IT-related modifications are appropriately authorized, tested, documented, implemented and disseminated, the change manage process should include the following:

- Classification and prioritization of changes and determination of the impact of changes;
- Roles and responsibilities of each relevant party, including IT functions and end-user departments, with adequate segregation of duties. This is to ensure that no single person can effect changes to the production environment without the review and approval of other authorized personnel;
- Program version controls and audit trails;
- Scheduling, tracking, monitoring and implementation of changes to minimize business disruption;
- Process for rolling-back changes to re-instate the original programs, system configuration or data in the event of production release problems; and
- Post implementation verification of the changes made (e.g. by checking the versions of major amendments).

7.3. Requested changes should be screened before acceptance to determine alternate methods of making the changes, the cost of changes and time requirements for programming activity. System analysts should assess the impact and validity of the proposed changes and all critical change requests should be set as priority.

7.4. The actual cause that led to the request for change should be identified and adequately documented. Formal reports on analysis for problems raised and status of change requests (including closed and outstanding) should be reported to senior management on a periodic basis.

7.5. Audit trail of all change requests should be maintained. Programmers' activities should be controlled and monitored, and all jobs assigned should also be closely monitored against target completion dates.

7.6. To enable unforeseen problems to be addressed in a timely and controlled manner, the BSI should establish formal procedures to manage emergency changes. Emergency changes should be approved by the information owner (for application system or production data-related changes) and other relevant parties at the time of change. If the change needs to be introduced as a matter of urgency and it is impracticable to seek the approval of the information owner, endorsement should be sought from the information owner after the implementation as soon as practicable (e.g. on the following business day).

7.7. Emergency changes should be logged and backed up (including the previous and changed program versions and data) so that recovery of previous program versions and data files is possible, if necessary. Emergency changes need to be reviewed by independent personnel to ensure that the changes are proper and do not have an undesirable impact on the production environment. They should be subsequently replaced by proper fixes through the normal acceptance testing and change management procedures.

7.8. Management should ensure that vendors permitted remote access to network resources are properly authorized. System logs showing activity on the system should be reviewed to ensure that unauthorized remote access has not taken place. Management may institute time of day restrictions for remote access, to limit the duration of time a user can access the network remotely (e.g. only during business

hours). Vendors utilizing dial in access should be verified through call back procedures and/or through the use of a modem that can be turned on when authorization has been granted by the system administrator.

7.9. Data patching could severely compromise the integrity of the database in production systems and should strictly be avoided. The BSI should adequately ensure the accuracy and reliability of its database and the integrity of its data. Good project management discipline requires validation of data input, data integrity testing, user sign-off, impact analysis and escalation of decision to senior management should be adopted to ensure accuracy and validity of data before live implementation.

8. SYSTEMS TESTING

8.1. A formal acceptance process should be established to ensure that only properly tested and approved systems are promoted to the production environment. System and user acceptance testing should be carried out in an environment separate from the production environment. Production data should not be used in development or acceptance testing unless the data has been desensitized (i.e. not disclosing personal or sensitive information) and prior approval from the information owner has been obtained. Performance testing should also be performed before newly developed systems are migrated to the production environment.

8.2. Sufficient testing is important to ensure that design and overall reliability of the application systems are in accordance with original specifications. Tests should be conducted using documented test plans that should encompass all predetermined data or processing problems and business scenarios.

8.3. User acceptance testing should be performed in a separate environment. All related users are responsible to ensure that adequate test scenarios are formulated and sufficiently tested. Successful test activities should be formally confirmed and accepted by users, before the modified programs can be transferred to the production environment.

9. SYSTEMS MIGRATION

9.1. A secured library for program pending migration to the production environment should be established. The secured library or quarantine area for all amended programs should only be accessible by the personnel who performed the migration process and restricted from the application programmers. This is to mitigate the risk of programmers changing the modified programs after user acceptance testing, but prior to the program migration.

9.2. Source compare procedure should be in place to verify changes and to ensure no unauthorized changes have been made. Modified programs should be compared to the authorized change documents to determine that only approved specification changes were implemented.

9.3. Updates or a version control for all applications should be maintained. Old versions of source codes[26] should be archived as contingency measure, with a clear indication

[26] **Source codes** are software program instructions written in format (language) readable by humans.

of the precise date, time and all necessary information while the latest version of the source codes and databases should be strictly protected. Version controls may also be implemented to ensure only authorized programs are migrated to quarantine and production environments.

10. SOURCE CODE CONVERSION AND MAINTENANCE

10.1. Conversion of source codes into object codes[27] should be adequately controlled in order to mitigate the risks of unauthorized changes and to ensure accurate and complete results. The conversion process should only be performed by designated personnel. In the case where the compiler programs or other systems development tools are used, it should be placed under restricted control and the access and execution rights are strictly monitored.

10.2. In cases where core applications are developed by vendors but the source codes were not released to the BSI, the institution's interest should be protected in the form of a written agreement. The agreement, generally known as escrow agreement, should allow the BSI to access the source programs under conditions, such as, but not limited to, discontinued product support or financial insolvency by the vendor. A third-party entity should be appointed to retain these programs and documents in escrow. However, it is important for the BSI to periodically determine that the source code maintained in escrow is up-to-date. If the BSI decides not to go into a source code escrow agreement, appropriate controls or contingency plans should be established as necessary, to continue adequate operation of the business or process the acquired program is supporting in case it becomes problematic, obsolete, or ceases to function.

11. SYSTEMS DOCUMENTATION

11.1 All standards and procedures on systems development and documentation on user manuals should be formally established and properly maintained to ensure consistency of approach. Accessibility to these documents should be strictly confined only to those who are authorized to receive such information in order for them to effectively discharge their duties.

11.2 Management should identify the type and level of documentation personnel must produce during each project phase. Project documentation of major IT projects, especially development and acquisition, should include project requests, feasibility studies, project plans, testing plans, etc. System documentation, which focuses on system analysis and design, should include system concept narratives, data flow charts, and database specifications. Application documentation should include application descriptions, programming flowcharts, and operations and user instructions. The documentation should be revised as needed throughout the project life cycle.

11.3 Documentation standards should identify primary documentation custodians and detail document authoring, approving, and formatting requirements. Personnel should document all changes to system, application, and configuration

[27] **Object codes** are software program instructions complied (translated) from source code into machine-readable formats.

documentation according to prescribed standards. Additionally, management should control access to documentation libraries with appropriate library and version controls.

11.4 All standards and documentation should be kept secured to prevent unauthorized access. The BSI should maintain a central storage (of either hardcopy or softcopy) of all standards and documentation onsite as well as in an offsite premise for contingency purposes. In the case where the application is developed by a vendor, management should ensure that adequate training and manuals are provided as part of the package, stated in writing and clearly understood by all parties. The BSI should also ensure complete and updated system documentation is provided.

12. POST-IMPLEMENTATION REVIEW

12.1. A post implementation review should be conducted at the end of a project to validate the application's operational performance, after it has begun to operate. The relative success of the project should be gauged by comparing planned and actual cost, benefits and completion time. If the planned objectives do not materialize, reasons should be reviewed and documented in a post implementation evaluation report that should be presented to senior management highlighting any operational or project management deficiencies noted.

12.2. The responsibilities for conducting post-implementation review can be assigned to the BSI's IT audit function. In larger IT organizations, formal quality assurance or change management groups may have primary responsibility for post-implementation reviews. In such cases, the IT auditor may choose not to perform a separate review but instead to participate in establishing the test criteria and evaluating results of any other independent reviews.

13. DISPOSAL

13.1. The BSI may sometimes need to remove surplus or obsolete hardware, software, or data. Primary tasks include the transfer, archiving, or destruction of data records. Management should transfer data from production systems in a planned and controlled manner that includes appropriate backup and testing procedures. The BSI should maintain archived repository of data in accordance with applicable record retention requirements and system documentation to facilitate reinstallation of a system into production, when necessary. Management should destroy data by overwriting old information or degaussing (demagnetizing) disks and tapes.

14. ROLE OF AUDIT, INFORMATION SECURITY AND QUALITY ASSURANCE OFFICERS

14.1 **Audit.** The BSI's auditors assist user departments, project managers, and system designers in identifying system control requirements and testing the controls during development and after implementation. Please refer to Item 6.1 of Appendix 75a for the detailed guidelines on audit's participation in the development, acquisition, and maintenance of major systems.

14.2 **Information Security.** The BSI should ensure that systems are developed, acquired and maintained with appropriate security controls. To do this, management

should ensure that – a) systems are developed and implemented with necessary security features enabled and based on established security control requirements; b) software is trustworthy by implementing appropriate controls in the different project phases; and c) appropriate configuration management and change control processes exist, including an effective patch management process. Management should establish security control requirements based on their risk assessment process evaluating the value of the information at risk and the potential impact of unauthorized access, damage or other threats.

14.3 **Quality Assurance.** Independent quality assurance function is a critical part of well-managed IT projects. Comprehensive quality assurance, risk management, and testing standards provide the best means to manage project risks and ensure IT projects, especially software, include expected functionality, security, and operability, as applicable.

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: IT Operations

1. INTRODUCTION

1.1. The evolving role IT plays in supporting the business function has become increasingly complex. IT operations – traditionally housed in a computer data center with user connections through terminals – have become more dynamic and include distributed environments, integrated applications, telecommunication options, internet connectivity, and an array of IT operating platforms[28]. With the advent of technology, even small BSIs have now become increasingly reliant on IT to achieve operational efficiency and deliver innovative products and services. Although some of these BSIs have developed their products and services in-house, many have relied on vendors and service providers to develop and operate these products and services.

1.2. The increasing dependency to IT of BSIs has consequently resulted to heightened risk exposures arising from their reliance on a variety of IT solutions and services and third-party relationships as well. It is also emphasized that risks involve more than IT and that controls include sound processes and well-trained people. To many BSIs, effective support and delivery from IT operations has become vital to the performance of most of their critical business lines. This necessitates the adoption of risk management processes that promote sound and controlled operation of IT environments to ensure that IT operations process and store information in a timely, reliable, secure, and resilient manner.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The BSI's Board and senior management are responsible for overseeing a safe, sound, controlled and efficient IT operating environment that supports the institution's goals and objective. Although they can delegate implementation and oversight of daily operations to IT management, final responsibility for these activities remains with the Board and senior management. Consequently, the Board and senior management are responsible for understanding the risks associated with existing and planned IT operations, determining the risk tolerance of the BSI, and establishing and monitoring policies for risk management.

On the other hand, IT operations management is primarily responsible in ensuring the BSI's current and planned infrastructure is sufficient to accomplish the strategic plans of senior management and the Board. To accomplish this objective, operations management should ensure the BSI has sufficient personnel (in knowledge, experience, and number), system capacity and availability, and storage capacity to achieve strategic objectives. Operations management should select or recommend IT

[28] IT **operating platform** includes the underlying computer system on which application programs run. A platform consists of an operating system, the computer system's coordinating program, which in turn is built on the instruction set for a processor or microprocessor, and the hardware that performs logic operations and manages data movement in the computer.

solutions that can meet strategic requirements with reduced resources to control capital expenditures and operating costs.

3. IT OPERATIONS STANDARDS

3.1. **Technology Inventory.** To effectively identify, assess, monitor, and manage the risks associated with IT operations, management should have a comprehensive understanding of the BSI's operations universe. Regardless of size, BSI management should perform and maintain an inventory of all its IT resources, recognize interdependencies of these systems and understand how these systems support the associated business lines. Management should ensure the inventory is updated on an on-going basis to reflect the BSI's IT environment at any point in time.

Appropriate documentation of infrastructure and data flow should be in place to facilitate risk identification, application of controls, and ongoing maintenance of information systems. At a minimum, said documentation should include among others, the following components:

- Hardware - Inventory should be comprehensive to include BSI's owned assets and equipment owned by other parties but located within the environment. To the extent possible, hardware items should be marked with a unique identifier, such as a bar code, tamper-proof tag, or other label.

- Software - There are at least three major categories of software the BSI should include in the software inventory: operating systems, application software, and back-office and environmental applications.

- Network Components and Topology[29] - Network management should develop and maintain high-level topologies that depict local area networks (LANs[30]), metropolitan area networks (MANs[31]) and wide area networks (WANs[32]). The topologies should have sufficient detail to facilitate network maintenance and troubleshooting, facilitate recovery in the event of a disruption and plan for expansion, reconfiguration, or addition of new technology.

- Data Flow Diagram - Management should also develop data flow diagrams to supplement its understanding of information flow within and between network segments as well as across the BSI's perimeter to external parties. Data flow diagrams are also useful for identifying the volume and type of data stored on various media. In addition, the diagrams should identify and differentiate

[29] A **network** is a group of two or more computers that are linked together. For example, networks allow users at different branches or different workstations to access the Internet, send and receive email, and share printers, applications, and data. A **network topology** pictorially describes the arrangement or architecture of a network, including its workstations and connecting communication lines.

[30] A **LAN** is a network that connects workstations in a relatively small geographic area, such as a building. Computers connected in a LAN are usually connected by cables, but they can also be connected wirelessly.

[31] A **MAN** is a network that usually spans a city or a large campus. A MAN usually interconnects a number of LANs using a high-capacity backbone technology, such as fiber-optical links, and provides up-link services to WAN and the internet.

[32] A **WAN** is a network that connects other networks together. WANs are typically complicated networks covering broad areas (i.e., any network that links across metropolitan, regional, or national boundaries) and allowing many computers and other devices to communicate and share data.

between data in electronic format, and in other media, such as hard copy or optical images.

- Media - Descriptive information should identify the type, capacity, and location of the media. It should also identify the location, type, and classification (public, private, confidential, or other) of data stored on the media. Additionally, management should document source systems, data ownership, back up frequency and methodology (tape, remote disk, compact disc (CD), or other), and the location of back-up media if other than at the primary off-site storage facility.

3.2. **Risk Assessment.** Once inventory is complete, management should employ a variety of risk assessment techniques to identify threats and vulnerabilities to its IT operations, covering among others, the following:

- Internal and external risks;
- Risks associated with individual platforms, systems, or processes as well as those of a systemic nature; and
- The quality and quantity of controls.

The risk assessment process should be appropriate to the BSI's IT risk profile. To the extent possible, the assessment process should quantify the probability of a threat or vulnerability and the financial consequences of such an event.

After the BSI identifies and analyzes the universe of risks, management should prioritize risk mitigation actions based on the probability of occurrence and the financial, reputational or legal impact to the institution. Management should prioritize the risk assessment results based on the business importance of the associated systems. The probability of occurrence and magnitude of impact provide the foundation for establishing or expanding controls for safe, sound, and efficient operations appropriate to the risk tolerance of the BSI.

3.3. **Risk Mitigation & Control Implementation**

3.3.1. **Policies, Standards and Procedures.** Board and management should enact policies, standards and procedures sufficient to address and mitigate the risk exposure of the BSI. The BSI should adopt minimum IT standards to establish measurable controls and requirements to achieve policy objectives. Procedures describe the processes used to meet the requirements of the BSI's IT policies and standards. Management should develop written procedures for critical operations which procedures should be updated and reviewed regularly. The scope of required procedures depends on the size, complexity and the variety of functions performed by the BSI's IT operations.

3.3.2. Controls Implementation

3.3.2.1. **Environmental Controls.** IT equipment should have a continuous uninterruptible power supply (UPS[33]). Management should configure the UPS to provide sufficient electricity within milliseconds to power equipment until there is an orderly shutdown or transition to the back-up generator. The back-up generator should generate sufficient power to meet the requirements of mission critical IT and environmental support systems. Similarly, IT operations centers should have independent telecommunication feeds from different vendors. Wiring configurations should support rapid switching from one provider to another without burdensome rerouting or rewiring.

Even small IT operations centers with modest IT equipment can contain a significant amount of computer cabling. Management should physically secure these cables to avoid accidental or malicious disconnection or severing. In addition, management should document wiring strategies and organize cables with labels or color codes to facilitate easy troubleshooting, repair, and upgrade.

Every operations center should have adequate heating, ventilation, and air conditioning (HVAC) systems in order for personnel and equipment to function properly. Organizations should plan their HVAC systems with the requirements of their IT systems in mind. Also, operations personnel should be familiar with written emergency procedures in the event of HVAC system disruption.

Water leaks can cause serious damage to computer equipment and cabling under raised floors. For this reason, operations centers should be equipped with water detectors under raised flooring to alert management of leaks that may not be readily visible. Management should also consider installing floor drains to prevent water from collecting beneath raised floors or under valuable computer equipment.

A variety of strategies are available for fire suppression. Ideally, the fire suppression system should allow operators time to shut down computer equipment and cover it with waterproof covers before releasing the suppressant.

Lastly, Management should consider using video surveillance and recording equipment in all or parts of the facility to monitor activity and deter theft. Management should also use inventory labels, bar codes, and logging procedures to control the inventory of critical and valuable equipment.

[33] **UPS** is a device that allows computer to keep running for at least a short time when the primary power source is lost. A UPS may also provide protection from power surges. A UPS contains a battery that "kicks in" when the device senses a loss of power from the primary source allowing the user time to save any data they are working on and to exit before the secondary power source (the battery) runs out. When power surges occur, a UPS intercepts the surge so that it doesn't damage the computer.

3.3.2.2. **Preventive Maintenance.** All maintenance activities should follow a predetermined schedule. A record of all maintenance activities should be maintained to aid management in reviewing and monitoring employee and vendor performance. Management should schedule time and resources for preventive maintenance and coordinate such schedule with production. During scheduled maintenance, the computer operators should dismount all program and data files and work packs, leaving only the minimum software required for the specific maintenance task on the system. If this is impractical, management should review system activity logs to monitor access to programs or data during maintenance. Also, at least one computer operator should be present at all times when the service representative is in the computer room.

In case a vendor performs computer maintenance online, operators should be aware of the online maintenance schedule so that it does not interfere with normal operations and processing. Operators and information security personnel should adhere to established security procedures to ensure they grant remote access only to authorized maintenance personnel at predetermined times to perform specific tasks.

Operators should maintain a written log of all hardware problems and downtime encountered between maintenance sessions. A periodic report on the nature and frequency of those problems is a necessary management tool, and can be valuable for vendor selection, equipment benchmarking, replacement decisions, or planning increased equipment capacity.

3.3.2.3. **Change Management**[34] **& Control.** Complex BSIs should have a change management policy that defines what constitutes a "change" and establishes minimum standards governing the change process. Simple BSIs may successfully operate with less formality, but should still have written change management policies and procedures.

All changes should flow through the oversight function, which may include appropriate representation from business lines, support areas, IT management, information security, and internal audit. In establishing a framework for managing change, a policy should be present describing minimum standards and including such factors as notification, oversight, and control. Control standards should address risk, testing, authorization and approval, timing of implementation, post installation validation, and back-out or recovery.

[34] **Change management** refers to the broad processes for managing organizational change. Change management encompasses planning, oversight or governance, project management, testing and implementation.

3.3.2.4. **Patch Management**[35]**.** Management should establish procedures to stay abreast of patches, to test them in a segregated environment, and to install them when appropriate. Change management procedures should require documentation of any patch installations. Management should develop a process for managing version control of operating and application software to ensure implementation of the latest releases. Management should also maintain a record of the versions in place and should regularly monitor the Internet and other resources for bulletins about product enhancements, security issues, patches or upgrades, or other problems with the current versions of the software.

3.3.2.5. **Conversions.** Conversions involve major changes to existing systems or applications, or the introduction of systems or data sets which may span multiple platforms. Consequently, they have a higher level of risk requiring additional, specialized controls. Conversions, if improperly handled, may result to corrupt data; hence, strong conversion policies, procedures, and controls are critical. Likewise, since the ramifications of conversion span IT operations, it is important for management to periodically re-evaluate all operations processes and consider the appropriateness of process re-engineering.

3.3.2.6. **Network Management Controls.** Network standards, design, diagrams and operating procedures should be formally documented, kept updated, communicated to all relevant network staff and reviewed periodically. Communications facilities that are critical to continuity of network services should be identified. Single points of failure should be minimized by automatic re-routing of communications through alternate routes should critical nodes or links fail.

The network should be monitored on a continuous basis to reduce the likelihood of network traffic overload and detect network intrusions. Powerful network analysis and monitoring tools, such as protocol analyzers, network scanning and sniffer tools, are normally used for monitoring network performance and detecting potential or actual intrusions. These powerful network tools should be protected from unauthorized usage (e.g. viewing of unencrypted sensitive information). The use of network tools should also be tightly restricted to authorized staff only and be subject to stringent approval and review procedures.

---

[35] A **patch** is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. In some special cases, updates may knowingly break the functionality, for instance, by removing components for that the update provider is no longer licensed. **Patch Management** is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

3.3.2.7. **Disposal of Media.** Management should have procedures for the destruction and disposal of media containing sensitive information. These procedures should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Furthermore, disposal procedures should recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since data can be recovered, additional disposal techniques should be applied to remove sensitive information.

3.3.2.8. **Imaging.** Management should ensure there are adequate controls to protect imaging processes, as many of the traditional audit and controls for paper-based systems may be reduced. Management should also consider issues such as converting existing paper storage files, integration of the imaging system into the organization workflow, and business continuity planning needs to achieve and maintain business objectives.

3.3.2.9. **Event/Problem Management.** Management should ensure appropriate controls are in place to identify, log, track, analyze, and resolve problems that occur during day-to-day IT operations. The event/problem management process should be communicated and readily available to all IT operations personnel. Management should ensure it trains all operations personnel to act appropriately during significant events. Employees should also receive training to understand event response escalation procedures.

Operations personnel should be properly trained to recognize events that could trigger implementation of the business continuity plan. Although an event may not initially invoke the plan, it may become necessary as conditions and circumstances change. Management should train and test BSI personnel to implement and perform appropriate business continuity procedures within the timeframes of the BCP. Operations personnel should properly log and record any events that trigger BCP response and document their ultimate resolutions.

3.3.2.10. **User Support/Help Desk.** User support processes and activities should ensure end users continuously have the resources and services needed to perform their job functions in an efficient and effective manner. In complex BSIs, the help desk function provides user support, which typically consists of dedicated staff trained in problem resolution, equipped with issue tracking software, and supported with knowledge-based systems that serve as a reference resource to common problems. In simple BSIs, user support may consist of a single person, a very small group, or a contract with a support vendor.

The help desk should record and track incoming problem reports, whether handled by live operators or automated systems.

Documentation in the tracking system should include such data as user, problem description, affected system (platform, application, or other), prioritization code, current status toward resolution, party responsible for resolution, root cause (when identified), target resolution time, and a comment field for recording user contacts and other pertinent information. The help desk should evaluate and prioritize issues to ensure the most critical problems receive prompt attention.

Help desk functions may also be supported by knowledge based-systems that provide support staff with action responses to common problems. Strong support functions continually update the knowledge based-systems with information obtained from vendors and from the experiences of help desk staff. Because attrition rates in the help desk function can be high, a knowledge based-system can ensure the BSI retains knowledge and facilitates the training and development of new employees.

Proper authentication of users is critical to risk management within the user support function. If the help desk uses a single authentication standard for all requests, it should be sufficiently rigorous to cover the highest risk scenarios. However, the BSI may choose to use different levels of authentication depending upon the problem reported, the type of action requested, or the platform, system, or data involved. If the help desk function is outsourced, management should determine the service provider's information access level, assign the functions it will perform, and ensure that security and confidentiality remain in place.

3.3.2.11. **Scheduling.** The BSI should implement policies and procedures for creating and changing job schedules and should supplement them with automated tools when cost effective. Sound scheduling practices and controls prevent degraded processing performance that can affect response time, cause delays in completing tasks, and skew capacity planning. Automated scheduling tools are necessary for large, complex systems to support effective job processing. Smaller and less complex IT systems generally have a standard job stream with little need for change.

3.3.2.12. **Systems and Data Back-up.** The BSI should ensure that sufficient number of backup copies of essential business information, software and related hardcopy documentations are available for restoration or critical operations. A copy of these information, documentation and software should also be stored in an off-site premise or backup site and any changes should be done periodically and reflected in all copies.

The BSI should back-up and store its data and program files in a secure off-site location to allow restoration of systems, applications, and associated data in the event normal processing is disrupted by a

disaster or other significant event. A full system backup should be periodically conducted and should at least consist of the updated version of the operating software, production programs, system utilities and all master and transaction files. The frequency of backup should depend on its criticality, but should be performed after critical modification or updates. Management should implement a storage solution that is manageable from an administrative perspective and usable and accessible from the customer and end-user perspectives to enable them to receive current, complete and accurate data. Storage solutions should be appropriately scalable to allow for future growth.

Written standards should document back-up methodologies, delineate responsibilities of appropriate personnel, and ensure uniform performance throughout the institution. Management should maintain inventories of back-up media stored off-site and periodically perform physical inventories to ensure all required back-up materials are available. Procedures should include verifying adherence to the back-up schedule and reviewing actual back-up copies for readability. Similarly, management should periodically test back-up copies by actually using them to restore programs and data.

All backup media should be properly labeled using standard naming conventions. Management should develop a rotation scheme that addresses varying storage durations as well as transportation and storage of multiple formats of media at the off-site storage location. Transportation to the backup site should be done in controlled and secured manner with proper authorization and record. Procedures for disposal of backup media should also be in place.

3.3.2.13. **Systems Reliability, Availability and Recoverability.**

- **System Availability**

  BSIs should achieve high systems availability (or near zero system downtime) for critical systems which is associated with maintaining adequate capacity, reliable performance, fast response time, scalability and swift recovery capability. Built-in redundancies for single points of failure should be developed and contingency plans should be tested so that business and operating disruptions can be minimized.

- **Technology Recovery Plan**

  Business resumption very often relies on the recovery of IT resources that include applications, hardware equipment and network infrastructure as well as electronic records. The technology requirements that are needed during recovery for individual business and support functions should be specified when the recovery strategies for the functions are determined.

Appropriate personnel should be assigned with the responsibility for technology recovery. Alternate personnel needs to be identified for key technology recovery personnel in case of their unavailability to perform the recovery process.

As unavailability of systems may result to disruptive impact on its operations, the BSI should develop an IT disaster recovery plan to ensure that critical application systems and technology services can be resumed in accordance with the business recovery requirements. In formulating an effective recovery plan, scenario analysis should be included to identify and address various types of contingency scenarios. Scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total inaccessibility of the primary data centre should be considered. To strengthen recovery measures relating to large scale disruptions and to achieve risk diversification, rapid operational and backup capabilities at the individual system or application cluster level should be implemented. Recovery and business resumption priorities must be defined accordingly. Specific recovery objectives including recovery time objective[36] (RTO) and recovery point objective[37] (RPO) should be established for systems and applications.

- **Alternate sites for technology recovery**

  The BSI should make arrangements for alternate and recovery sites[38] for their business functions and technology in the event the business premises, key infrastructure and systems supporting critical business functions become unavailable. A recovery site geographically separate from the primary site must be established to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site. 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. Recovery strategies and technologies such as on-site redundancy and real-time data replication could be explored to enhance the BSI's recovery capability.

  The recovery site could either be an in-house backup premise that has a redundant hardware system located away from the computer center, or a third-party recovery facility provider that requires formal subscription to its service, or a combination of

[36] **RTO** refers to the required time taken to recover an IT system from the point of disruption.

[37] **RPO** refers to the acceptable amount of data loss for an IT system should a disaster occur.

[38] **Recovery site** is an alternate location for processing information (and possibly conducting business) in an emergency.

both solutions. The recovery facility should be at a distance that would protect it from damage from any incident occurring at the primary site. Ideally, it should be on different electrical power and telecommunication switches, and free from the same disaster. The BSI should ensure that the IT systems at the recovery sites are:

- Compatible with the BSI's primary systems (in terms of capacity and capability) to adequately support the critical business functions; and
- Continuously updated with current version of systems and application software to reflect any changes to the BSI's system configurations (e.g. hardware or software upgrades or modifications).

In case where a third-party recovery facility is used, there should be a written contract agreement that is legally binding. The agreement should specifically identify the conditions under which the recovery facility may be used and specify how customers would be accommodated if simultaneous disaster conditions occur to several customers of the recovery facility provider. The recovery facility should allow the BSI to use its services until it achieves a full recovery from the disaster and resumption of activity at the BSI's own facility.

The BSI which outsources critical systems to offshore service providers is heavily dependent on the stability and availability of cross-border network links. To minimize impact to business operations in the event of a disruption (e.g. due to earthquake), cross-border network redundancy with strategies such as engagement of different network service providers and alternate network paths may be instituted.

- **Disaster Recovery Testing**

The BSI should always adopt pre-determined recovery actions that have been tested and endorsed by management. The effectiveness of recovery requirements and the ability of BSI's personnel in executing or following the necessary emergency and recovery procedures should be tested and validated at least annually.

Various scenarios which include total shutdown or inaccessibility of the primary data center, as well as component failure at the individual system or application cluster level should be included in disaster recovery tests. Inter-dependencies between and among critical systems should be included in the tests. BSIs whose networks and systems are linked to specific service providers and vendors, should consider conducting bilateral or multilateral recovery testing.

Business users should be involved in the design and execution of comprehensive test cases so as to obtain assurance that recovered systems function accordingly. The BSI should also participate in disaster recovery tests of systems hosted overseas. Periodic testing and validation of the recovery capability of backup media should be carried out and assessed for adequacy and effectiveness. Backup tapes and disks containing sensitive data should be encrypted before they are transported offsite for storage.

3.4. Risk Monitoring

3.4.1. **Service Level Agreement (SLA).** BSI Management of IT functions should formulate an SLA with business units which will measure the effectiveness and efficiency of delivering IT services. Measurable performance factors include system availability and performance requirements, capacity for growth, and the level of support provided to users, resource usage, operations problems, capacity, response time, personnel activity, as well as business unit and external customer satisfaction. Adequate procedures should be in place to manage and monitor delivery of committed services.

3.4.2. **Control Self-Assessments[39] (CSAs).** The BSI may consider the conduct of periodic CSAs to validate the adequacy and effectiveness of the IT control environment. They also facilitate early identification to allow management to gauge performance, as well as the criticality of systems and emerging risks. Depending on the complexity of the BSI's IT risk profile, the content and format of the CSAs may be standardized and comprehensive or highly customized, focusing on a specific process, system, or functional area. IT operations management may collaborate with the internal audit function in creating the templates used. Typically, the CSA form combines narrative responses with a checklist. The self-assessment form should identify the system, process, or functional area reviewed, and the person(s) completing and reviewing the form. CSA's however, are not a substitute for a sound internal audit program. Management should base the frequency of CSA the risk assessment process and coordinate the same with the internal audit plan.

3.4.3. **Performance Monitoring.** The BSI should implement a process to ensure that the performance of IT systems is continuously monitored and exceptions are reported in a timely and comprehensive manner. The performance monitoring process should include forecasting capability to enable problems to be identified and corrected before they affect system performance. Monitoring and reporting also support proactive systems management that can help the BSI position itself to meet its current needs and plan for periods of growth, mergers, or expansion of products and services.

BSI Management should also conduct performance monitoring for outsourced IT solutions as part of a comprehensive vendor management program. Reports from service providers should include performance metrics, and identify the

[39] CSA is a technique used to assess risk and control strength and weaknesses against a control framework.

root causes of problems. Where service providers are subject to SLAs, management should ensure the provider complies with identified action plans, remuneration, or performance penalties.

3.4.4. **Capacity Planning.** Management should monitor IT resources for capacity planning including platform processing speed, core storage for each platform's central processing unit, data storage, and voice and data communication bandwidth[40]. Capacity planning should be closely integrated with the budgeting and strategic planning processes. It also should address personnel issues including staff size, appropriate training, and staff succession plans. This process should help the preparation of workload forecasts to identify trends and to provide information needed for the capacity plan, taking into account planned business initiatives. Capacity planning should be extended to cover back-up systems and related facilities in addition to the production environment.

4. ROLE OF IT AUDIT

4.1. The BSI's IT audit function should regularly assess the effectiveness of established controls within the IT operations environment through audits or other independent verification. Audits provide independent assessments rendered by qualified individuals regarding the effective functioning of operational controls.

[40] Bandwidth is a terminology used to indicate the transmission or processing capacity of a system or of a specific location in a system (usually a network system) for information (text, images, video, sound). It is usually defined in bits per second (bps)

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: IT Outsourcing / Vendor Management

1. INTRODUCTION

1.1. With globalization and advancement in IT, BSIs increasingly rely on services provided by other entities to support an array of IT-related functions. The ability to outsource IT systems and process enables a BSI to manage costs, obtain necessary expertise, expand customer product offerings, and improve services. While outsourcing offers a cost-effective alternative to in-house capabilities, it does not reduce the fundamental risks associated with IT or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information and regulatory action remain. Because the functions are performed by an organization outside the BSI, the risks may be realized in a different manner than if the functions were inside resulting in the need for well-structured process to properly manage risks and ensure that the interest of customers will not be compromised.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The responsibility for the oversight and management of outsourcing activities and accountability for all outsourcing decisions continue to rest with the BSI's Board and senior management. They should establish and approve enterprise-wide policies, appropriate to the IT risk profile of the institution. This framework should govern the end-to-end perspective of outsourcing process and shall provide the basis for management to identify, measure, monitor, and control the risks associated with IT-related outsourcing arrangements.

3. IT OUTSOURCING / VENDOR RISK MANAGEMENT PROGRAM

3.1 **Risk Assessment.** Prior to entering into an outsourcing plan, the BSI should clearly define the business requirements for the functions or activities to be outsourced, assess the risk of outsourcing those functions or activities and establish appropriate measures to manage and control the identified risks. Risk assessment should take into consideration the criticality of the services to be outsourced, the capability of the technology service provider (TSP)[41] and the technology it will use in delivering the outsourced service. Such assessment should be made periodically on existing arrangements as part of the outsourcing program and review process of the BSI.

3.2 **Service Provider Selection.** Before selecting a service provider, the BSI should perform appropriate due diligence of the provider's financial soundness, reputation,

[41] TSPs include a wide range of entities including but not limited to affiliated entities, non-affiliated entities, and alliances of companies providing technology products and services. These services may include but not limited to the following: a) information and transaction processing and settlement activities that support banking functions; b) electronic banking-related services; c) Internet-related services; d) security monitoring; e) systems development and maintenance; f) aggregation services; and g) digital certification services. Other terms used to describe TSPs include vendors and external/outsourced service providers.

managerial skills, technical capabilities, operational capability and capacity in relation to the services to be outsourced. The depth and formality of the due diligence performed may vary depending on the nature of the outsourcing arrangement and the BSI's familiarity with the prospective service providers. Contract negotiation should be initiated with the service provider determined to best meet the business requirements of the BSI.

Due diligence undertaken during the selection process should be documented and reviewed periodically, using the most recent information, as part of the monitoring and control processes of outsourcing.

3.3 **Outsourcing Contracts.** The contract is the legally binding document that defines all aspects of the servicing relationship and one of the most important controls in outsourcing process. It should be clearly written and sufficiently detailed to provide assurances for performance, reliability, security, confidentiality and reporting. Before signing a contract, management should:

- Ensure the contract clearly defines the rights and responsibilities of both parties and contains or supported by adequate and measurable service level agreements;
- Ensure contracts with related entities clearly reflect an arms-length relationship and costs and services are on terms that are substantially the same, or at least as favorable to the BSI, as those prevailing at the time for comparable transactions with non-related third parties;
- Choose the most appropriate pricing method for the BSI's needs;
- Ensure service provider's physical and data security standards meet or exceed the BSI's standards. Any breach in security should be reported by the service provider to the BSI;
- Engage legal counsel to review the contract; and
- Ensure the contract contains the minimum provisions required under existing BSP rules and regulations, like access by BSP to systems and databases outsourced, and the same does not include any provisions or inducements that may adversely affect the BSI (i.e. extended terms, significant increases after the first few years, substantial cancellation penalties)

Each agreement should allow for renegotiation and renewal to enable the BSI to retain an appropriate level of control over the outsourcing and the right to intervene with appropriate measures to meet its legal and regulatory obligations. The agreement should also acknowledge BSP's supervisory authority over the BSI and the right of access to information on the BSI and the service provider.

Some service providers may contract with third-parties in providing IT services to the BSI. The extent to which subcontractors perform additional services should be limited to peripheral or support functions while the core services should rest with the main service provider. The BSI should retain the ability to maintain similar control over its outsourcing risks when a service provider uses subcontractors in the course of rendering the IT-related services. Agreements should have clauses setting out the rules and limitations on subcontracting. To provide accountability, it may be beneficial for the BSI to include a provision specifying that the contracting service provider shall remain fully responsible with respect to parts of the services which

were further outsourced to subcontractors. It should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.

An annual review of the outsourcing agreements should be performed to assess whether the agreements should be renegotiated and renewed to bring them in line with current market standards and to cope with changes in their business strategies. When renegotiating contracts, the BSI should ensure that the provider delivers a level of service that meets the needs of the institution over the life of the contract.

3.4 **Service Level Agreement (SLA).** SLAs formalize the performance standards against which the quantity and quality of service should be measured. Management should include SLAs in its outsourcing contracts to specify and clarify performance expectations, as well as establish accountability for the outsourced activity. The BSI should link SLA to the provisions in the contract regarding incentives, penalties and contract cancellation in order to protect themselves in the event the service provider failed to meet the required level of performance.

Management should closely monitor the service provider's compliance with key SLA provision on the following aspects, among others:

- Availability and timeliness of services;
- Confidentiality and integrity of data;
- Change control;
- Security standards compliance, including vulnerability and penetration management;
- Business continuity compliance; and
- Help desk support.

SLAs addressing business continuity should measure the service provider's contractual responsibility for backup, record retention, data protection, and maintenance and testing of disaster recovery and contingency plans. Neither contracts nor SLAs should contain any extraordinary provisions that would exempt the service provider from implementing its contingency plans (outsourcing contracts should include clauses that discuss unforeseen events for which the BSI would not be able to adequately prepare).

3.5 **Ongoing Monitoring**

3.5.1. **Monitoring Program.** As outsourcing relationships and interdependencies increase in materiality and complexity, the BSI needs to be more proactive in managing its outsourcing relationships. It should establish a monitoring program to ensure service providers deliver the quantity and quality of services required by the contract. The resources to support this program will vary depending on the criticality and complexity of the system, process, or service being outsourced.

The program should employ effective mechanisms to monitor key aspects of the outsourcing relationship and the risk associated with the outsourced activity, particularly the following:

- contract/SLA performance;
- material problems encountered by the service provider which may impact the BSI;
- financial condition and risk profile; and
- business continuity plan, the results of testing thereof and the scope for improving it.

To increase the effectiveness of monitoring mechanisms, management should periodically classify service provider relationships to determine which service providers require closer monitoring. Relationships with higher risk classification should receive more frequent and stringent monitoring for due diligence, performance (financial and/or operational), and independent control validation reviews.

Personnel responsible for monitoring activities should have the necessary expertise to assess the risks and should maintain adequate documentation of the process and results thereof. Management should use such documentation when renegotiating contracts as well as developing business continuity planning requirements.

Reports on the monitoring and control activities of the BSI should be prepared or reviewed by its senior management and provided to its Board. The BSI should also ensure that any adverse development arising from any outsourced activity is brought to the attention of the senior management, or the Board, when warranted, on a timely basis. Actions should be taken to review the outsourcing relationship for modification or termination of the agreement.

3.5.2. **Financial Condition of Service Providers.** The BSI should have an on-going monitoring of the financial condition of its service providers as financial problems may jeopardize the quality of its service and possibly the integrity of the data in its possession. In the event management recognizes that the financial condition of the provider is declining or unstable, more frequent financial reviews of said provider are warranted.

3.5.3. **General Control Environment of the Service Provider.** The BSI should also implement adequate measures to ensure service providers are only given access to the information and systems that they need in order to perform their function. Management should restrict their access to BSI's systems, and appropriate access controls and monitoring should be in place between the service provider's systems and the BSI.

3.6 **Business Continuity Planning Consideration.** The BSI should integrate the provider's BCP into its own plan, communicate functions to the appropriate personnel, and maintain and periodically review the combined plan. It should ensure that service provider tests its plan annually and notify the institution of any resulting modifications.

3.7 **Compliance with BSP Regulations.** The BSI should ensure that appropriate up-to-date records relevant to its outsourcing arrangements are maintained in its premises

and kept available for inspection by the BSP Examiners. The outsourcing agreement should explicitly provide a clause allowing BSP and BSIs' internal and external auditors to review the operations and controls of the service provider as they relate to the outsourced activity.

In addition to the general guidelines on outsourcing contracts stated in Item No. 3.3 of this Appendix, the BSIs intending to outsource must comply with existing BSP rules and regulations on outsourcing.

4. EMERGING OUTSOURCING MODELS

4.1. With continued and fast growth of technology, outsourcing of IT-related systems and processes has been a constant theme among BSIs. While outsourcing strategy allows BSIs to achieve growth targets, operational efficiency and cost savings, this also exposes them to various levels and kinds of risks. Potential risk exposures and other significant supervisory concerns are further heightened by the emergence of flexible and innovative outsourcing models (i.e. shared-services, offshoring and cloud computing).

4.2. Due mainly to the perceived implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention. Currently, the most widely accepted definition of cloud computing is as follows –

> *A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.*[42]

4.3. In general, cloud computing is a migration from owned resources to shared resources in which client users receive IT services, on demand, from third-party service providers a.k.a. Cloud Service Providers (CSP) via the Internet "cloud." This emerging model allows BSIs the option to move from a capital-intensive approach to a more flexible business model that lowers operational costs. Cloud computing technologies can be implemented in a wide variety of architectures, under different service and deployment models, and can coexist with other technologies and software design approaches. The four (4) cloud deployment models include the following:

- ***Private Cloud*** – A private cloud is operated solely for an institution and is closely related to the existing IT outsourcing models in the marketplace, but can be an institution's internal delivery model as well.
- ***Public Cloud*** – A public cloud is owned and operated by a CSP that delivers services to the general public or a large industry group via the internet or other computer network using a multi-tenant platform.
- ***Community Cloud*** – It is a private-public cloud with users having a common connection or affiliation, such as a trade association, the same industry or a

[42] National Institute of Standards Technology, *The NIST Definition of Cloud Computing: Special Publication 800-145, 2011, www.nist.gov/itl/cloud/*

common locality. It allows a CSP to provide cloud tools and applications specific to the needs of the community.

- ***Hybrid Cloud*** – This model composes two or more clouds (private, community or public). A hybrid cloud leverages on the advantage of the other cloud models, thus, providing a more optimal user experience.

4.4. Cloud computing is perceived to play an increasingly important role in a wide range of development initiatives, including among others, offering small to medium-sized BSIs critical access to infrastructure and computational resources that would otherwise be out of their financial reach or are too complex to manage. While the advantages of adopting an outsourced cloud-based component are undeniable, the fact remains that cloud computing also creates disruptive possibilities and potential risks. Many of the threats identified are not necessarily unique to the cloud environment. In fact, risks such as potential data loss, poor management by a service provider, service interruption and unauthorized access to sensitive data are also applicable to traditional forms of outsourcing. Cloud computing, however, adds new dimensions to the traditional outsourcing risks, thus, the vulnerabilities and the probability of the risk event occurring is amplified. BSIs should be fully aware of the unique attributes and risks associated with cloud computing, particularly in the following areas: (Details are shown in the attached Annex "A")

- Legal and Regulatory Compliance;
- Governance and Risk Management;
- Due Diligence;
- Vendor Management/Performance and Conformance;
- Security and Privacy;
- Data Ownership and Data Location and Retrieval;
- Business Continuity Planning.

4.5. Among the four (4) cloud models, the private cloud deployment is most similar to traditional outsourcing model, thus, offers the least amount of new risks and security challenges. Implementation of this model is allowed subject to compliance with existing BSP rules and regulations on outsourcing. Adoption of community and hybrid cloud deployment models may also be allowed with prior BSP approval, subject to the following:

- Compliance with existing BSP rules and regulations on outsourcing;
- Implementation of more robust risk management systems and controls required for these types of arrangements;
- Issues set out in the attached Annex "A" are properly addressed prior to executing the plans; and
- BSP may be allowed to perform onsite validation prior to implementing the cloud computing arrangement/s.

4.6. However, given the increased probability of risk & exposure to potential issues related to business operations, confidentiality and compliance which are critical in the financial service industry, the BSP, at present, would only allow the use of public cloud computing model for non-core operations and business processes (e.g. email, office productivity, collaboration tools, claims and legal management, etc.) which

do not directly involve sensitive BSI and customer data. BSP approval of public cloud deployment model for non-core operations shall be subject to the same conditions in item 4.5 above. Core operations and business processes whose importance is fundamental in ensuring continuous and undisturbed operation of IT systems used to directly perform banking and financial services (e.g. CA/SA, Loans, Trust and Treasury systems, ATM switch operations, electronic delivery systems and systems used to record banking operations) are not allowed to use public cloud computing service. Distinguishing whether a particular actual operation or business is "core" or "non-core" and classifying the data (e.g. confidential, critical, sensitive, public) associated with the system or application are, therefore, significant considerations in determining permissibility of public cloud model for this type of operation or process.

4.7. BSIs should consult BSP before making any significant commitment on cloud computing.

5. ROLE OF IT AUDIT

5.1. The BSI should conduct a regular, comprehensive audit of its service provider relationships. The audit scope should include a review of controls and operating procedures that help protect the BSI from losses due to irregularities and willful manipulations. Such responsibility can be assigned to the BSI's IT audit function. In case the BSI has no technical audit expertise, the non-technical audit methods can provide minimum coverage and should be supplemented with comprehensive external IT audits.

Despite its many potential benefits, cloud computing also brings with it potential areas of concern, when compared with computing environments found in traditional data centers. Some of the more fundamental concerns include the following:

- **Legal and Regulatory Compliance**

  Important considerations for any BSI before deploying a cloud computing model include clearly understanding the various types of laws and regulations that potentially impact cloud computing initiatives, particularly those involving confidentiality, visibility, data location, privacy and security controls and records management. The nature of cloud computing may increase the complexity of compliance with applicable laws and regulations because customer data may be stored or processed offshore. The BSI's ability to assess compliance may be more complex and difficult in an environment where the Cloud Service Provider (CSP) processes and stores data overseas or comingles the BSI's data with data from other customers that operate under diverse legal and regulatory jurisdictions. The BSI should understand the applicability of local laws and regulations and ensure its contract with a CSP specify its obligations with respect to the BSIs' responsibilities for compliance with relevant laws and regulations. CSP's processes should not compromise compliance with the following, among others:

  - Law on Secrecy of Deposits (R.A. No. 1405);
  - Foreign Currency Deposit System (R.A. 6426)
  - Anti-Money Laundering Act, particularly on data/file retention;
  - Electronic Commerce Act (R.A. 8792);
  - Data Privacy Law;
  - Cybercrime Prevention Act;
  - General Banking Laws (R.A. No. 8791); and
  - Regulations concerning IT risk management, electronic banking, consumer protection, reporting of security incidents and other applicable BSP issuances, rules and regulations.

  Lastly, the CSP should grant BSP access to its cloud infrastructure to determine compliance with applicable laws and regulations and assess soundness of risk management processes and controls in place.

- **Governance and Risk Management**

  The use of outsourced cloud services to achieve the BSI's strategic plan does not diminish the responsibility of the Board of Directors and management to ensure that the outsourced activity is conducted in a safe and sound manner and in compliance with applicable laws and regulations. The BSI Management should consider overall business and strategic objectives prior to outsourcing the specific IT operations to the cloud computing platform. A Board-approved outsourcing policy and rationale for outsourcing to the cloud environment should be in place to ensure that the Board is fully apprised of all the risks identified.

  Outsourcing to a CSP can be advantageous to a BSI because of potential benefits such as cost reduction, flexibility, scalability, improved load balancing, and speed. However, assessing and managing risk in systems that use cloud services can be a formidable

challenge due mainly to the unique attributes and risks associated with a cloud environment especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality as well as legal issues such as regulatory compliance, auditing and data offshoring. Cloud computing may require more robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a CSP, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment of elements specific to the service. Vendor management, information security, audits, legal and regulatory compliance, and business continuity planning are key elements of sound risk management and risk mitigation controls for cloud computing. As with other service provider offerings, cloud computing may not be appropriate for all BSIs.

- **Due Diligence**

  The due diligence in selecting a qualified CSP is of paramount importance to ensure that it is capable of meeting the BSI's requirements in terms of cost, quality of service, compliance with regulatory requirements and risk management. Competence, infrastructure, experience, track record, financial strength should all be factors to consider. When contemplating transferring critical organizational data to the cloud computing platform, it is critical to understand who and where all of the companies and individuals that may touch the BSI's data. This includes not only the CSP, but all vendors or partners that are in the critical path of the CSP. Background checks on these companies are important to ensure that data are not being hosted by an organization that does not uphold confidentiality of information or that is engaging in malicious or fraudulent activity. Business resiliency and capability to address the BSI's requirements for security and internal controls, audit, reporting and monitoring should also be carefully considered.

- **Vendor Management/Performance and Conformance**

  It is always important to thoroughly review the potential CSP's contract terms, conditions and Service Level Agreement (SLA). This is to ensure that the CSP can legally offer what it has verbally committed to and that the cloud risk from the CSP's service offerings is within the determined level of acceptable risk of the BSI. The SLA should ensure adequate protection of information and have details on joint control frameworks. It should also define expectations regarding handling, usage, storage and availability of information, and specify each party's requirements for business continuity and disaster recovery. At a minimum, the SLA should cover the provisions required under existing rules and regulations on outsourcing.

  A vendor management process should be in place that proactively monitors the performance of the CSP on an ongoing basis. This is also to guarantee availability and reliability of the services provided and ability to provide consistent quality of service to support normal and peak business requirements. If a BSI is using its own data centre, it can mitigate and prepare for outages. However, if it is using a cloud computing service, it has to put all its trust in the cloud service provider delivering on its SLA. This requires that SLA has sufficient means to allow transparency into the way a CSP operates, including the provisioning of composite services which is a vital ingredient for effective oversight of system security and privacy by the BSI.

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Collection and analysis of available data about the state of the system should be done regularly and as often as needed by the BSI to manage security and privacy risks, as appropriate for each level of the organization involved in decision making. Transition to public cloud services entails a transfer of responsibility to the CSP for securing portions of the system on which the BSI's data and applications operate. To fulfill the obligations of continuous monitoring, the organization is dependent on the CSP, whose cooperation is essential, since critical aspects of the computing environment are under its complete control.

Cloud services that allow CSP to further outsource or subcontract some of its services may also heighten concerns, including the scope of control over the subcontractor, the responsibilities involved (e.g., policy and licensing arrangements), and the remedies and recourse available should problems occur. A CSP that hosts applications or services of other parties may involve other domains of control, but through transparent authentication mechanisms, appear to the BSI to be that of the CSP. Requiring advanced disclosure of subcontracting arrangements, and maintaining the terms of these arrangements throughout the agreement or until sufficient notification can be given of any anticipated changes, should be properly enforced.

Additionally, the complexity of a cloud service can obscure recognition and analysis of incidents. The CSP's role is vital in performing incident response activities, including incident verification, attack analysis, containment, data collection and preservation, problem remediation, and service restoration. Each layer in a cloud application stack, including the application, operating system, network, and database, generates event logs, as do other cloud components, such as load balancers and intrusion detection systems; many such event sources and the means of accessing them are under the control of the cloud provider. It is important that the CSP has a transparent response process and mechanisms to share information with the BSI during and after the incident. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought. The geographic location of data is a related issue that can impede an investigation, and is a relevant subject for contract discussions. Revising the BSI's incident response plan to address differences between the organizational computing environment and the cloud computing environment is also a prerequisite to transitioning applications and data to the cloud.

Lastly, to effectively monitor services including risk and risk mitigation associated with the use of a CSP, the BSI and the CSP should agree in advance that former shall have accessibility to the CSP to audit and verify the existence and effectiveness of internal and security controls specified in the SLA. The BSI's audit policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing. It may also be necessary to augment the internal audit staff with additional training and personnel with sufficient expertise in evaluating shared environments and virtualized technologies. In addition, the parties may also agree on the right to audit clause via external party as a way to validate other control aspects that are not otherwise

accessible or assessable by the BSI's own audit staff. Ideally, the BSI should have control over aspects of the means of visibility to accommodate its needs, such as the threshold for alerts and notifications, and the level of detail and schedule of reports.

- **Security and Privacy**

  Security and privacy concerns continue to be a major issue within a cloud computing model. Given the obvious sensitivity of data and the regulated environment within which they operate, BSIs utilizing cloud systems, need to have an assurance that any data exposed on the cloud is well protected. They may need to revise their information security policies, standards, and practices to incorporate the activities related to a CSP. They should also have an understanding of and detailed contracts with SLAs that provide the desired level of security to ensure that the CSP is applying appropriate controls. In certain situations, continuous monitoring of security infrastructure may be necessary for BSIs to have a sufficient level of assurance that the CSP is maintaining effective controls.

  It is important that BSIs maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data is restricted appropriately through effective identity and access management. A multi-tenant cloud deployment, in which multiple clients share network resources, increases the need for data protection through encryption and additional controls such as virtualization mechanisms to address the risk of collating organizational data with that of other organizations and compromising confidential information through third-party access to sensitive information. Verifying the data handling procedures, adequacy and availability of backup data, and whether multiple service providers are sharing facilities are important considerations. If the BSI is not sure that its data are satisfactorily protected and access to them is appropriately controlled, entering into a cloud service arrangement may not be suitable.

  Storage of data in the cloud could increase the frequency and complexity of security incidents. Therefore, management processes of the BSI should include appropriate notification procedures; effective monitoring of security-related threats, incidents and events on both BSI's and CSP's networks; comprehensive incident response methodologies; and maintenance of appropriate forensic strategies for investigation and evidence collection.

- **Data Ownership and Data Location and Retrieval**

  The BSI's ownership rights over the data must be firmly established in the contract to enable a basis for trust and privacy of data. Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the CSP acquires no rights or licenses through the agreement, to use the BSI's data for its own purposes; and that the CSP does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the CSP.

  One of the most common challenges in a cloud computing environment is data location. Use of an in-house computing center allows the BSI to structure its computing environment and to know in detail where data is stored and what safeguards are used to

protect the data. In contrast, the dynamic nature of cloud computing may result in confusion as to where information actually resides (or is transitioning through) at a given point in time, since multiple physical locations may be involved in the process. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. One of the main compliance concerns is the possible transborder flows of data which may impinge upon varying laws and regulations of different jurisdictions.

To address the above constraints, the BSI should pay attention to the CSP's ability to isolate and clearly identify its customer data and other information system assets for protection. Technical, physical and administrative safeguards, such as access controls, often apply. Likewise, such concerns can be alleviated if the CSP has some reliable means to ensure that an organization's data is stored and processed only within specific jurisdictions. Lastly, external audits and security certificates can mitigate the issues to some extent.

- **Business Continuity Planning**

  The BCP in a BSI involves the recovery, resumption, and maintenance of the critical business functions, including outsourced activities. Due to the dynamic nature of the cloud environment, information may not immediately be located in the event of a disaster. Hence, it is critical to ensure the viability of the CSP's business continuity and disaster recovery plans to address broad-based disruptions to its capabilities and infrastructure. The plans must be well documented and tested. Specific responsibilities and procedures for availability, data backup, incident response and recovery should be clearly understood and stipulated. Recovery Time Objectives should also be clearly stated in the contract. It is critical for the BSI to understand the existence and comprehensiveness of the CSP's capabilities as well as its level of maturity to ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner. Other BCP-related concerns which must be addressed by the BSI and CSP include the following:

  - Prioritization arrangements in case of multiple/simultaneous disasters;
  - Retention of onsite and offsite back-up (Whether to maintain an up-to-date backup copy of data at the BSI's premises or stored with a second vendor that has no common points of failure with the CSP); and
  - Ability to synchronize documents and process data while the client-BSI is offline.

IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Products and Services

1. INTRODUCTION

1.1. Continuing technological innovation and competition among existing financial institutions and new entrants have contributed to a wide array of electronic products and services (e-services) available to customers. These products and services have been widely adopted by BSIs in recent years and are now a component of most institutions' business strategy. Electronic delivery of services can have many benefits for BSIs and their customers and can also have implications on financial condition, risk profile, and operating performance. The emergence of e- services may contribute to improving the efficiency of the banking and payment system, reducing the cost of retail transactions nationally and internationally and expanding the target customers beyond those in traditional markets. Consequently, BSIs are therefore becoming more aggressive in adopting electronic capabilities that include sophisticated marketing systems, remote-banking capabilities, and stored value programs.

1.2. Notwithstanding the significant benefits of technological innovation, the rapid development of electronic capabilities carries risks as well as benefits and it is important that these risks are recognized and managed by BSIs in a prudent manner to promote safe and secure e-services and operations. The basic types of risks generated by e-services are not new, the specific ways in which some of the risks arise, as well as the magnitude of their impact may be new for BSIs and supervisors. While existing risk management guidelines remain applicable to e-services, such guidelines must be tailored, adapted and, in some cases, expanded to address the specific risk management challenges created by the characteristics of such activities. As the industry continues to address technical issues associated with e-services, including security challenges, a variety of innovative and cost efficient risk management solutions are likely to emerge. These solutions are also likely to address issues related to the fact that BSIs differ in size, complexity and risk management culture and that jurisdictions differ in their legal and regulatory frameworks.

2. ROLES AND RESPONSIBILITIES

2.1. **Board of Directors (Board) and Senior Management.** The Board is expected to take an explicit, informed and documented strategic decision as to whether and how the BSI is to provide e-services to their customers. The Board and senior management should establish effective management oversight of the risks associated with these activities, including the establishment of specific accountability, policies and controls to manage these risks. Senior management oversight processes should operate on a dynamic basis in order to effectively intervene and correct any material systems problems or security breaches that may occur.

The Board should ensure that plans to offer e-services are consistent and clearly integrated within corporate strategic goals. The BSI should also ensure that it does not offer new e-services or adopt new technologies unless it has the necessary expertise to provide competent risk management oversight. Management and staff

expertise should be commensurate with the technical nature and complexity of the BSI's applications and underlying technologies.

The Board and senior management should ensure that the operational and security risk dimensions of the BSI's business strategies on e-services are appropriately considered and addressed. The provision of e-services may significantly modify and/or even increase traditional business risks. As such management should take appropriate actions to ensure that the BSI's existing risk management, security control, due diligence and oversight processes for outsourcing relationships are appropriately evaluated and modified to accommodate e-services.

BSI management should assess the impact of the implementation and ongoing maintenance of e-services. These areas should be monitored and analyzed on an ongoing basis to ensure that any impact on the BSI's financial condition and risk profile resulting from e-services is appropriately managed and controlled. Management should evaluate e-services acceptance vis-à-vis the performance to the its goals and expectations through periodic review of reports tracking customer usage, problems such as complaints and downtime, unreconciled accounts or transactions initiated through the system, and system usage relative to capacity. Insurance policies may also need to be updated or expanded to cover losses due to system security breaches, system downtime, or other risks from e-services.

2.2. **Compliance Officer.** The compliance officer or its equivalent should be aware and informed of all relevant laws and regulatory requirements relative to the offering of e-services, including those of other countries where they also intend to deliver cross-border e-services. BSI management should ensure that these requirements are complied with to minimize legal and compliance risks and other negative implications.

3. RISK MANAGEMENT SYSTEM

3.1. The BSI should carefully evaluate the offering a new e-service to customers to ensure that Management fully understands the risk characteristics and that there are adequate staffing, expertise, technology and financial resources to launch and maintain the service. A formal business strategy for introducing new service should be in place and form part of the BSI's overall strategy. The BSI should also perform regular assessments to ensure that its controls for managing identified risks remain proper and adequate.

3.2. The underlying risk management processes for e-services should be integrated into the BSI's overall risk management framework and the existing risk management policies and processes should be evaluated to ensure that they are robust enough to cover the new risks posed by current or planned activities. Relevant internal controls and audit as required in BSI's risk management system should also be enforced and carried out as appropriate for its e-services. Regular review of the relevant policies and controls should be performed to ascertain that these remain appropriate to the risks associated with such activities.

3.3. The BSI should adjust or update, as appropriate, its information security program in the light of any relevant changes in technology, the sensitivity of its customer

information and internal or external threats to information. The BSI should ensure that the related information security measures and internal control are installed, regularly updated, monitored and are appropriate with the risks associated with their products and services.

4. RISK MANAGEMENT CONTROLS

4.1. **Security Controls.** The BSI should recognize that e-services should be secured to achieve a high level of confidence with both customers and business. It is the responsibility of BSI management to provide adequate assurances that transactions performed and information flowed through the electronic delivery channels are properly protected. For this reason, the BSI should maintain a strong and comprehensive security control system. As such, in addition to the information security standards in Appendix 75b, the BSI should also provide the following controls specific for e-services:

4.1.1. **Account Origination and Customer Verification.** The BSI should use reliable methods for originating new customer accounts. Potentially significant risks may arise when it accepts new customers through the internet or other electronic channels. Thus, the BSI should ensure that in originating new accounts using electronic channels, the KYC requirement which involves a face-to-face process is strictly adhered to.

4.1.2. **Authentication.** The BSI should use reliable and appropriate authentication methods to validate and verify the identity and authorization of customers. The determination of the appropriate and reasonable authentication methods to be used in specific e-services application should be based on management's assessment of the risk posed by the electronic delivery channels adopted, types and amounts of transactions allowed, the sensitivity and value of customer information and transaction and the ease of using the authentication method.

The use of single factor authentication alone is generally considered not adequate for sensitive communications, high value transactions, third party transfers or privileged user access (i.e., network administrators[43]). Multi-factor techniques are necessary in those cases unless there are adequate security measures, risk mitigating controls (e.g. in some authorized institutions, third-party transfers are restricted to accounts that have been pre-registered) and effective monitoring mechanism to detect suspicious transactions and unusual activities. As authentication methods continue to evolve, the BSI should monitor, evaluate and adopt industry sound practice in this area to ensure appropriate changes are implemented for each transaction type and level of access based on the current and changing risk factors.

The authentication process should be consistent with and support the BSI's overall security and risk management programs. An effective authentication process should have customer acceptance, reliable performance, scalability to

[43] **Network administrator** is the individual responsible for the installation, management and control of a network.

accommodate growth and interoperability with existing systems and future plans as well as appropriate policies, procedures and control.

4.1.3. **Non-Repudiation**[44]. As customers and merchants originate an increasing number of transactions, authentication and encryption become increasingly important to ensure non-repudiation of transactions. In such cases, the BSI should consider implementing non-repudiation controls in the form of digital signatures, collision-free hash value of the entire transaction or unique authorization code that will provide conclusive proof of participation of both the sender and receiver in an online transaction environment. Public key infrastructure[45], digital signature[46], digital certificate[47] and certification authority[48] arrangements can be used to impart an enhanced level of security, authentication and authorization which can uniquely identify the person initiating transaction, detect unauthorized modifications and prevent subsequent disavowal.

4.1.4. **Authorization Controls and Access Privileges.** Specific authorization and access privileges should be assigned to all individuals, agents or systems, which conduct activities on e-services. No individual agent or system should have the authority to change his or her own authority or access privileges in the e-services authorization database. Any addition of an individual, agent or system or changes to access privileges should be duly authorized by an authenticated source empowered with adequate authority and subject to suitable and timely oversight and audit trails.

All systems that support e-services should be designed to ensure that they interact with a valid authorization database. Appropriate measures should be in place in order to make authorization databases reasonably resistant to tampering. Authenticated e-services sessions should remain secure throughout the full duration of the session. In the event of a security lapse, the session should require re-authentication. Controls should also be in place to prevent changes to authorization levels during e-services sessions and any attempts to alter authorization should be logged and brought to the attention of management.

---

[44] **Non-repudiation** is a means of ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

[45] **Public Key Infrastructure (PKI)** refers to the use of public key cryptography in which each customer has a key pair (i.e. unique electronic value called a public key and a mathematically-related private key). The private key is used to encrypt (sign) a message that can only be decrypted by the corresponding public key or to decrypt message previously encrypted with the public key. The public key is used to decrypt message previously encrypted (signed) using an individual's private key or to encrypt a message so that it can only be decrypted (read) using the intended recipient's private key.

[46] **Digital certificate** is a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be.

[47] **Digital Certificate** is the electronic equivalent of an ID card that authenticates the originator of digital signature.

[48] **Certification Authority (CA)** is the organization that attests using a digital certificate that a particular electronic message comes from a specific individual or system.

No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. Only employees with proper authorization and whose official duties necessitate access to such data, applications, system resources or facilities should be allowed to access confidential information and use system resources solely for legitimate purposes.

4.1.5. **Confidentiality and Integrity of Information, Transactions and Records.** The BSI should ensure that appropriate measures are in place to ascertain the accuracy, completeness and reliability of e-services transactions, records and information that are either transmitted over the internal and external networks or stored in BSI's internal systems. Common practices used to maintain data integrity include the following:

- E-services transactions should be conducted in a manner that make them highly resistant to tampering throughout the entire process;
- E-services records should be stored, accessed and modified in a manner that make them highly resistant to tampering;
- E-services transaction and record-keeping processes should be designed in a manner as to make it virtually impossible to circumvent detection of unauthorized changes.
- Adequate change control policies, including monitoring and testing procedures, should be in place to protect against any system changes that may erroneously or unintentionally compromise controls or data reliability; and
- Any tampering with e-services transactions or records should be detected by transaction processing, monitoring and record keeping functions.

The BSI should take appropriate measures to preserve the confidentiality of key e-services information commensurate with the sensitivity of the information being transmitted and/or stored in databases. It should ensure that all intelligent electronic devices that capture information do not expose/store information such as the PIN number or other information classified as confidential and must also ensure that a customer's PIN number cannot be printed for any reason whatsoever. In addition, the BSI must provide safe-to-use intelligent electronic devices and ensure that customers are able to make safe use of these devises at all times.

The BSI should implement appropriate technologies to maintain confidentiality and integrity of sensitive information, in particular customer information. Cryptographic technologies can be used to protect the confidentiality and integrity of sensitive information. The BSI should choose cryptographic technologies that are appropriate to the sensitivity and importance of information and the extent of protection needed and, only those that are making use of internationally recognized cryptographic algorithms where the strengths of the algorithms have been subjected to extensive tests. In cases when the information is transmitted over public network, the BSI should consider the need to apply strong end-to-end encryption to the transmission of sensitive information.

To ensure adequate protection and secrecy of cryptographic keys whether they are master keys, key encrypting keys or data encrypting keys, no single individual should know entirely what the keys are or have access to all the constituents making up these keys. All keys should be created, stored, distributed or changed under the most stringent conditions. Likewise, use of these keys should be logged and provided with timely oversight.

4.1.6. **Application Security.** The BSI should ensure an appropriate level of application security in its electronic delivery systems. In selecting system development tools or programming languages for developing e-services application systems, it should evaluate the security features that can be provided by different tools or languages to ensure that effective application security can be implemented. In selecting an e-services system developed by a third party, the BSI should take into account the appropriateness of the application security of the system. It should test new or enhanced applications thoroughly using a general accepted test methodology in a test environment prior to implementation.

The BSI should consider the need to have customers confirm sensitive transactions like enrolment in a new on-line service, large funds transfers, account maintenance changes, or suspicious account activity. Positive confirmations for sensitive on-line transactions provide the customer with the opportunity to help catch fraudulent activity. The BSI can encourage customer participation in fraud detection and increase customer confidence by sending confirmations of certain high-risk activities through additional communication channels such as the telephone, e-mail, or traditional mail.

Comprehensive and effective validation of input parameters (including user-supplied data and database queries that may be submitted by the users' computers) should be performed on server side. This prevents intentional invalid input parameters from being processed by the e-services system that may result in unauthorized access to data, execution of commands embedded in the parameters or a buffer overflow attack[49]. Moreover, e-services systems should operate with the least possible system privileges.

Error messages generated by the application system for e-services customers should not reveal details of the system which are sensitive. Errors should be appropriately logged. Similarly, the HTML[50] source code on the production web server should not contain sensitive information such as any references or comments that relate to the design features of the web application code.

The mechanism for managing an active e-services session should be secure. Web pages containing sensitive information should not be cached in the temporary files of browsers. The application should ideally prohibit the customers' browsers from memorizing or displaying the user IDs and

[49] **Buffer overflow attack** is a method of overloading a predefined amount of space in a buffer, which can potentially overwrite and corrupt memory in data.

[50] **Hypertext Markup Language (HTML)** is a set of codes that can be inserted into text files to indicate special interfaces, inserted images, and links to the hypertext documents.

passwords previously entered by customers and the web pages previously accessed by customers.

When a known vulnerability related to the e-services application system is identified or reported, a review of the relevant program source code should be conducted as appropriate to ensure that the vulnerability is appropriately addressed. A security standard may be defined for the purpose of system development and code review. For third-party developed systems, the patches provided by vendors from time to time should be appropriately applied to these systems.

Hidden directories that contain administrative pages or sensitive information of the web site should either be removed from the production web server or protected by effective authentication and access control mechanisms. Back-up files and common files should be removed from the production servers or the structure of file directories to prevent access by unauthorized users. A periodic security review of the structure of file directories and access controls of the files is necessary to ensure that all sensitive files are appropriately protected and not exposed through the web applications.

4.1.7. **Infrastructure and Security Monitoring.** The BSI should establish an appropriate operating environment that supports and protects systems on e-services. It should proactively monitor systems and infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. The BSI should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-services systems, servers, databases, and applications. The attached Annex "A" provides for the minimum security measures for e-services facilities.

The BSI should put in place effective monitoring mechanisms to detect in a timely manner suspicious online transactions and unusual activities. A sound monitoring system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords or other unauthorized activities. In particular, the monitoring mechanism for personal e-services should be able to detect cases similar to the following:

- False or erroneous application information, large check deposits on new e-services accounts, unusual volume or size of funds transfers, multiple new accounts with similar account information or originating from the same internet address, and unusual account activity initiated from a foreign internet address;
- Multiple online transfers are made to the same unregistered third-party account within a short period of time especially if the amount transferred is close to the maximum amount allowed or the value exceeds a certain amount; and
- Change of a customer's correspondence address shortly followed by transactions which may indicate potential fraudulent activities such as opening of an e-service account online, a request for important documents (e.g. cheque book, new e-banking password, credit card/ATM PIN) to be

mailed to that address, increase of fund transfer limits, or a sudden increase of fund transfers made to unregistered third parties.

The BSI's monitoring staff should be promptly alerted by its monitoring mechanism if suspicious online transfers and unusual activities are initiated. In these cases, the BSI should, as soon as practicable, check with the account holders of these transactions or activities. Consideration should also be given to notifying personal customers immediately through an alternative automated channel (such as messages sent to mobile phones or e-mail accounts of customers) of online transfers made to unregistered third parties, online transfers exceeding certain amount limits, or detected unusual activities related to their accounts.

4.1.8. **Controls Over Fund Transfers.** The BSI that relies solely on single factor authentication for e-services should consider restricting third-party transfer only to accounts that have been pre-registered by the customer. As an alternative, customers may be allowed to register third-party accounts online but the registration should be effected only after a period when a written confirmation is expected to have reached the customer.

To mitigate fraud risk, the BSI may establish amount limits on transactions initiated through the e-services application, or may monitor transactions above specified limits, depending on the type of account (e.g., consumer vs. corporate). Such limits or similar monitoring systems may help detect unusual account activity that may indicate fraudulent transactions or other suspicious activity. Other safeguards to manage the risk of unauthorized third-party transfers include the following, among others:

- Maximum daily or transaction limits should be imposed on online transfers to unregistered third-parties;
- A second factor authentication should be employed before a customer can effect online transfers to unregistered third-parties; and
- Two-factor authentication should be implemented for corporate or institutional e-services that allow transfers to unregistered third-party accounts.

4.1.9. **Audit Trail.** The BSI should ensure that comprehensive logs are maintained to record all critical e-services transactions to help establish a clear audit trail and promote employee and user accountability. Audit logs should be protected against unauthorized manipulation and retained for a reasonable period (e.g. three months) to facilitate any fraud investigation and any dispute resolution if necessary. In instances where processing systems and related audit trails are the responsibility of a third-party service provider, the BSI should ensure that it has access to relevant audit trails maintained by the service provider in accordance with existing standards. In particular, clear audit trails should exist under the following types of e-services transactions:

- the opening, modification or closing of a customer's account;
- any transaction with financial consequences;
- any authorization granted to a customer to exceed a limit; and

- any granting, modification or revocation of systems access right orprivileges.

4.1.10. **Segregation of Duties.** As in any traditional process, segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems. The BSI management should ensure that duties are adequately separated and transaction processes are designed in a manner that no single person could initiate, approve, execute and enter transactions into a system that would enable fraudulent actions to be perpetrated and concealed. Segregation should also be maintained between (a) those developing and those administering the systems; and (b) those initiating static data (including web page content) and those responsible for verifying its integrity. E-services systems should be tested to ensure that segregation of duties cannot be bypassed.

4.1.11. **Website Information and Maintenance.** Because the BSI's website is available on an ongoing basis to the general public, appropriate procedures should be established to ensure accuracy and appropriateness of its information. Key information changes and updates (such as deposit, loan and foreign exchange rates), are normally subject to documented authorization and dual verification. Procedures and controls to monitor and verify website information frequently may help prevent any inadvertent or unauthorized modifications or content that could lead to reputational damage or violations of advertising, disclosure, or other compliance requirements.

In addition, some BSIs provide various tools and other interactive programs to enable customers to submit online application or provide resources for them to research available options associated with BSI's products and services on-line. To protect the BSI from potential liability or reputational harm, it should test or otherwise verify the accuracy and appropriateness of these tools and programs.

The BSI should carefully consider how links to third-party Internet Web sites are presented. "Hyperlinks[51]" may imply an endorsement of third-party products, services, or information that could lead to implicit liability for the BSI. The BSI should provide disclaimers when such links take the customer to a third-party web site to ensure that they clearly understand any potential liabilities arising out of any such cross-marketing arrangements or other agreements with third parties. Any links to sites offering non-deposit, investment or insurance products must comply with existing regulations. Links to other sites should be verified regularly for accuracy, functionality, and appropriateness.

The BSI should manage the risk associated with fraudulent emails or websites which are designed to trick its customers into revealing private details such as account numbers or e-services passwords. To this end, the BSI should consider educating customers the ways to ensure that they are

[51] **Hyperlink** is an item on a webpage, that, when selected, transfers the user directly to another location in a hypertext document or to another webpage, perhaps on a different machine.

communicating with the official website and that they will not be required to access the BSI's transactional e-services portal through hyperlinks embedded in e-mails unless the website is validated by legitimate digital certificate.

Additionally, the BSI should exercise care in selecting its website name(s) in order to reduce possible confusion with those of other Internet sites. It should periodically scan the Internet to identify sites with similar names and investigate any that appear to be posing as the institution. Suspicious sites should be reported to appropriate law enforcement agencies and regulatory authorities.

4.2. **Administrative and Management Controls**

4.2.1. **Administration of E-Services Accounts.** The BSI should ensure that adequate controls are in place to minimize the risks of e-services accounts being opened by fraudsters without the knowledge of the real customers. It is recommended that the BSI issues a written confirmation to the customer concerned and prohibit the online transfers to unregistered third parties until the institution is satisfied that the customer has received the confirmation. It should also perform adequate identity checks when customer requests a change in his account information or other contact details.

4.2.2. **Service Availability and Business Continuity.** The BSI should have the ability to deliver e-services to all end-users and be able to maintain such availability in all circumstances within a reasonable system response time in accordance with its terms and conditions and anticipated customer expectations. Performance criteria for each critical e-service should be established and service levels should be monitored against these criteria. Appropriate measures should be taken to ensure that e-services systems and the interfaces with the internal systems can handle the projected transaction volume and future growth in transactions.

Appropriate business continuity and contingency plans for critical e-services processing and delivery systems should be in place and regularly tested. Contingency plans should set out a process for restoring or replacing e-services processing capabilities, reconstructing supporting transaction information, and include measures to be taken to resume availability of critical e-services systems and applications in the event of a business disruption.

4.2.3. **Incident Response and Management.** The BSI should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-services during or outside office hours. A communication strategy should be developed to adequately address the reported concerns and an incident response team should be established to manage and respond to the incident in accordance with existing standards enumerated in Appendix 75b.

4.2.4. **Outsourcing Management.** Increased reliance upon partners and third party service providers to perform critical e-services functions lessens BSI

management's direct control. Accordingly, a comprehensive process for managing the risks associated with outsourcing and other third-party dependencies is necessary to ensure that:

- The BSI fully understands the risks associated with entering into an outsourcing or partnership arrangement for its e-services systems or applications;
- An appropriate due diligence review of the competency and financial viability of any third-party service provider or partner is conducted prior to entering into any contract for e-services;
- The contractual accountability of all parties to the outsourcing or partnership relationship is clearly defined. For instance, responsibilities for providing information to and receiving information from the service provider should be clearly defined;
- All outsourced e-services systems and operations are subject to risk management, security and privacy policies that meet the BSI's own standards;
- Periodic independent internal and/or external audits are conducted of outsourced operations to at least the same scope required if such operations were conducted in-house; and
- Appropriate contingency plans for outsourced e-services activities exist.

Complete guidelines for managing outsourcing relationships and third party dependencies are enumerated in Appendix 75e.

4.3. **Consumer Protection**

4.3.1. **Customer Privacy and Confidentiality.** The BSI should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the institution is providing electronic products and services. Misuse or unauthorized disclosure of confidential customer data exposes the entity to both legal and reputation risk. To meet these challenges concerning the preservation of privacy of customer information, the BSI should make reasonable endeavours to ensure that:

- The BSI's customer privacy policies and standards take account of and comply with all privacy regulations and laws applicable to the jurisdictions to which it is providing e-services;
- Customers are made aware of the BSI's privacy policies and relevant privacy issues concerning use of e-services;
- Customers may decline ("opt out") from permitting the BSI to share with a third party for cross-marketing purposes any information about the customer's personal needs, interests, financial position or banking activity; and
- Customer data are not used for purposes beyond which they are specifically allowed or for purposes beyond which customers have authorized. The BSI's standards for customer data use must be met when third parties have access to customer data through outsourcing relationships.

4.3.2. **Information Disclosure for E-Services.** The BSI should comply with all legal requirements relating to e-services, including the responsibility to provide its customers with appropriate disclosures and to protect customer data. Failure to comply with these responsibilities could result in significant compliance, legal, or reputation risk for the BSI.

The BSI should set out clearly in its terms and conditions the respective rights and obligations between the BSI and its customers. These terms and conditions should be fair and balanced to both parties. In addition, it is required to provide its customers with a level of comfort regarding information disclosures or transparencies, protection of customer data and business availability that they can expect when using traditional banking services. To minimize operational, legal and reputational risks associated with e-services activities, the BSI should make adequate disclosures of information and take appropriate measures to ensure adherence to customer privacy and protection requirements. Annex "B" provides for the minimum disclosure requirements of BSIs.

4.3.3. **Consumer Awareness.** Customer education is a key defense against fraud, identity theft and security breach. Therefore, the BSI should pay special attention to the provision of easy to understand and prominent advice to its customers on security precautions for e-services. To be effective, the BSI should maintain and continuously evaluate its consumer awareness program. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials, the number of clicks on information security links on websites, the number of inquiries, etc. Annex "C" provides for the minimum Consumer Awareness Program that the BSI should convey to its customers.

4.3.4. **Complaints Resolution.** The BSI may receive customer complaint either through an electronic medium or otherwise, concerning an unauthorized transactions, loss or theft in the e-services account. Therefore, it should ensure that controls are in place to review these notifications and that an investigation is initiated as required. The BSI should also establish procedures to resolve disputes arising from the use of the e-services.

4.4. **Cross-Border E-Banking Activities**

4.4.1. Before a BSI initiates cross-border e-services, its management should conduct appropriate risk assessment and due diligence to ensure that it can adequately manage the attendant risks. It must also comply with any applicable laws and regulations, both the home country as well as those of any foreign country that may assert jurisdiction over e-services that are directed at its residents. Further, the BSI should ensure that it has an effective and ongoing risk management program for its cross-border e-services activities;

4.4.2. Before engaging in transactions involving cross-border e-services with foreign customers, the BSI should ensure that adequate information is disclosed on its Web site to allow potential customers to make a determination of the BSI's identity, home country, and whether it has the relevant regulatory license(s)

before it establishes the relationship. This information will help improve transparency and minimize legal and reputational risk associated with the offering of cross border e-services.

5. INDEPENDENT ASSESSMENT

5.1. An appropriate independent audit function is also an important component of a BSI's monitoring mechanisms. The audit coverage should be expanded commensurate with the increased complexity and risks inherent in e-services and should include the entire process as applicable (i.e. network configuration and security, interfaces to legacy systems, regulatory compliance, internal controls, support activities performed by third-party providers etc.).

5.2. The BSI should also make arrangements for independent assessments to be conducted on its systems before the launch of the relevant services or major enhancements to existing services. The person(s) (i.e. the assessor) contracted by the BSI to perform independent assessment should have, and be able to demonstrate, the necessary expertise in the relevant fields. He/she should be independent from the parties that develop or administer the system and should not be involved in the operations to be reviewed or in selecting or implementing the relevant control measures to be reviewed. He/she should be able to report findings freely and directly to the authorized BSI senior management.

5.3. Subsequent to an initial independent assessment, the BSI should conduct risk assessment at least every two years or when there are substantial changes to determine if further independent assessment should be required and the frequency and scope of such independent assessment. Any substantial changes to the risk profile of the services being provided, significant modifications of the network infrastructure and applications, material system vulnerabilities or major security breaches are to be taken into consideration in the risk assessment.

6. APPLICABILITY

6.1. These guidelines are intended for all electronic products and services offered by BSIs to their customers. These are focused on the risks and risk management techniques associated with electronic delivery channels to protect customers and general public. It should be understood, however, that not all the customer protection issues that have arisen in connection with new technologies are specifically addressed in subject guidelines. Additional issuances may be issued in the future to address other aspects of consumer protection as the financial service environment through e-services evolves.

SECURITY CONTROLS ON SPECIFIC ELECTRONIC SERVICES AND CHANNELS

In providing banking/financial services via electronic channels, such as ATM, internet and mobile devices, the BSI must consider customer's convenience in using the facilities, including the effectiveness of the display on electronic menu, particularly on customer's instructions selection menu in order to avoid any error and loss in transactions. In electronic services which involve physical equipment like ATMs, the BSI must implement physical security control on equipments and rooms from the danger of theft, sabotage and other criminal actions by unauthorized parties. It must perform routine monitoring to ensure security and comfort of customers using electronic service.

Automated Teller Machine (ATM)

1. To minimize/prevent ATM frauds and crimes, the BSI, at a minimum, implement the following security measures with respect to its ATM facilities:

    - Locate ATM's in highly visible areas;
    - Provide sufficient lighting at and around the ATMs;
    - Where ATM crimes (e.g., robbery, vandalism, skimming) are high in a specific area or location, the BSI should install surveillance camera or cameras which shall view and record all persons entering the facility. Such recordings shall be preserved by the BSI for at least thirty (30) days;
    - Implement ATM programming enhancements like masking/non-printing of card numbers;
    - Educate customers by advising them regularly of risks associated with using the ATM and how to avoid these risks;
    - Conduct and document periodic security inspection at the ATM location;
    - Educate BSI personnel to be responsive and sensitive to customer concerns; and
    - Post a clearly visible sign near the ATM facility which, at a minimum, provides the telephone numbers of the BSI as well as other BSIs' hotline numbers for other cardholders who are allowed to transact business in the ATM, and police hotlines for emergency cases.

2. The BSI must study and assess ATM crimes to determine the primary problem areas. Procedures for reporting ATM crimes should also be established. Knowing what crimes have occurred will aid the BSI in recognizing the particular problem and to what degree it exists so that it can implement the necessary preventive measures. In this connection, all BSIs are encouraged to share information involving ATM fraud cases to deter and prevent proliferation of the crime.

Online Internet Financial Services

1. Assurance should be provided that online login access and transactions performed over the internet are adequately protected and authenticated. In addition, customers should be adequately educated on security measures that must be put in place to uphold their interests in the online environment.

2. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. The BSI should implement physical and logical access security to allow only authorized personnel to access its systems. Appropriate processing and transmission controls should also be implemented to protect the integrity of systems and data.

3. There should be a mechanism to authenticate official website to protect customers from spoofed or faked websites. The BSI should determine what authentication technique to adopt to provide protection against these attacks. For wireless applications, it should adopt authentication protocols that are separate and distinct from those provided by the wireless network operator.

4. Monitoring or surveillance systems should be implemented to alert BSI of any erratic system activities, transmission errors or unusual online transactions. A follow-up process should be established to verify that these issues or errors are adequately addressed subsequently. High resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment) should be maintained to meet customers' expectations. Measures to plan and track capacity utilization as well as guard against online attacks should be established.

5. As more customers log into BSI's website to access their accounts and conduct a wide range of financial transactions for personal and business purposes, a suite of measures must be established to protect customers' interests in using online systems. Furthermore, customers should be educated on the risks of using online financial services before they subscribe to such services. Ongoing education must be available to raise the security awareness of customers to protect their systems and online transactions.

Mobile and Phone Financial Services

1. For electronic services using mobile phone, the BSIs must ensure the security of transactions by implementing the followings, among others:
   - Employment of a SIM Toolkit with end-to-end encryption feature from hand phones to m-banking servers, to protect data transmission in m-banking; and
   - Adoption of dual authentications process (i.e. MPIN) to ensure that the party initiating the transaction is the owner of the device and is authorized to perform such transaction.

2. For phone banking and other financial services, the BSI must ensure the security of transactions, by implementing the followings, among others:
   - The service shall not be used for transactions with high value or risk;
   - All IVR conversations shall be recorded, including customer's phone number, transaction detail, etc;
   - The service shall use reliable and secure authentication methods; and
   - The use of customer authentication method such as PIN and password for financial transactions.

Other Mobile Online and Payment Services

1. Mobile online and payment services are extensions of the online financial services which are offered by the BSI and accessible from the internet via computers, laptops and similar devices. Security measures which are similar to those of online financial and payment systems should also be implemented on the mobile online services and payment systems. A risk assessment should be conducted to identify possible fraud scenarios and appropriate measures should be established to counteract payment card fraud via mobile devices.

2. The BSI may require customers to download its mobile online services and payment applications directly from third party repositories (e.g. Apple store, Google Play and Windows Market Place) on to mobile devices. Customers must be able to verify the integrity and authenticity of the application prior to its download. The BSI should also be able to check the authenticity and integrity of the software being used by the customers.

3. As mobile devices are susceptible to theft and loss, there must be adequate protection of sensitive data used for mobile online services and payments. Sensitive data should be encrypted to ensure the confidentiality and integrity of these data in storage, transmission and during processing.

4. Customers should be educated on security measures to protect their own mobile devices from theft and loss as well as viruses and other errant software which cause malicious damage and harmful consequences.

Point of Sale Devices

1. Point of Sale (POS)/Electronic Data Capture (EDC) enable electronic fund transfer from customer's account to acquirer's or merchant's account for payment of a transaction. The party providing POS terminal must always increase the physical security around the vicinity of such POS terminal and on the POS terminal itself, among others, by using POS terminal that minimizes the possibility of interception on such terminal or in its communication network.

2. The BSI deploying POS devices at merchant locations must familiarize the merchant with the safe operation of the device. The acquiring institution must ensure that the POS devices as well as other devices that capture information do not expose/store information such as the PIN number or other information classified as confidential. It must also ensure that a customer's PIN number cannot be printed at the point of sale for any reason whatsoever.

3. Operators of point of sale devices are encouraged to work towards interoperability of cards from other schemes.

Electronic Payment Cards (ATM, Credit and Debit Cards)

1. Payment cards allow cardholders the flexibility to make purchases wherever they are. Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including payment kiosks and POS terminals. In addition to

counterfeit/skimmed cards, fraudulent activities associated with payment cards include lost/stolen cards, card-not-received and card-not-present transactions.

2. The BSI providing payment card services should implement adequate safeguards to protect sensitive payment card data. Sensitive payment card data should be encrypted to ensure the confidentiality and integrity of these data in storage, transmission and during processing. Pending the required adoption of EMV chip-cards by 01 January 2017, all BSIs engaged in the payment card business should consider implementing the following measures to mitigate exposure from skimming attacks:

    - Installation of anti-skimming solutions on ATM and POS machines to detect the presence of foreign devices placed over or near a card entry slot;
    - Establishment of detection and alert mechanisms to appropriate personnel for follow-up response and action;
    - Implementation of tamper-resistant keypads to ensure that no one can identify which buttons are being pressed by customers;
    - Implementation of appropriate measures to prevent shoulder surfing of customers' PINs; and
    - Conduct video surveillance of activities at these machines and maintain the quality of CCTV footage.

3. New payment cards sent to customers via courier should only be activated upon obtaining the customer's instruction. Online transactions should only be allowed if authorized by the customers. Authentication of customers' sensitive static information, such as personal identification number (PIN) or passwords, should be performed by the card issuer and not by third party payment processing service providers. Appropriate security mechanisms should also be implemented for card-not-present transactions via internet to reduce fraud risk associated with this type of transaction.

4. To enhance payment card security, cardholders should be notified promptly via transaction alerts on withdrawals/charges exceeding customer-defined thresholds made on their payment cards. The transaction alert should include information such as source and amount of the transaction to assist customers in identifying a genuine transaction.

5. Fraud detection systems with behavioral scoring and correlation capabilities should be implemented to identify and curb fraudulent activities. Risk management parameters should be calibrated according to risks posed by cardholders, nature of transactions or other risk factors to enhance fraud detection capabilities. Follow-up actions for transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns should be instituted. These transactions should be investigated into and the cardholder's authorization obtained prior to completing the transaction.

DISCLOSURE REQUIREMENTS

1. General Requirement

BSIs offering electronic products and services (e-services) should adopt responsible privacy policies and information practices. They should provide disclosures that are clear and readily understandable, in writing, or in a form the consumers may print and keep.

BSIs should also ensure that consumers who sign-up for a new e-service are provided with disclosures (e.g. pamphlet) informing him of his rights as a consumer.

At a minimum, the following disclosures should be provided to protect consumers and inform them of their rights and responsibilities:

- Information on the duties of the BSI and customers;
- Information on who will be liable for unauthorized or fraudulent transactions;
- Mode by which customers will be notified of changes in terms and conditions;
- Information relating to how customers can lodge a complaint, and how a complaint may be investigated and resolved;
- Disclosures that will help consumers in their decision-making (e.g., PDIC insured, etc.);
- For internet environment, information that prompt in the BSI's website to notify customers that they are leaving the BSI's website and hence they are not protected by the privacy policies and security measures of the BSI when they hyperlink to third party's website.

2. Disclosure Responsibility

- Compliance officers should review BSI's disclosure statements to determine whether they have been designed to meet the general and specific requirements set in the regulation;
- For BSIs that advertise deposit products and services on-line, they must verify that proper advertising disclosures are made (e.g. whether the product is insured or not by the PDIC; fees and charges associated with the product or services, etc.). Advertisements should be monitored to determine whether they are current, accurate, and compliant;
- For BSIs that issue various products like stored value cards, e-wallets, debit cards and credit cards, they must provide information to consumers regarding the features of each of these products to enable consumers to meaningfully distinguish them. Additionally, consumers would find it beneficial to receive information about the terms and conditions associated with their usage. Example of these disclosures include:
  - PDIC insured or non-insured status of the product;
  - Fees and charges associated with the purchase, use or redemption of the product;

- Liability for lost;
- Expiration dates, or limits on redemption; and
- Toll-free telephone number for customer service, malfunction and error resolution.

- Whenever e-services are outsourced to third parties or service providers, the BSI should ensure that the vendors comply with the disclosure requirements of the BSP.

ELECTRONIC SERVICES CONSUMER AWARENESS PROGRAM

To ensure security of transactions and personal information in electronic delivery channels, consumers should be oriented of their roles and responsibilities which, at a minimum, include the following:

1. Internet Products and Services

   a) Secure Login ID and Password or PIN
      - Do not disclose Login ID and Password or PIN
      - Do not store Login ID and Password or PIN on the computer.
      - Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 6 digits in length.

   b) Keep personal information private.
      - Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, bank account number or e-mail address — unless the one collecting the information is reliable and trustworthy.

   c) Keep records of online transactions.
      - Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
      - Review and reconcile monthly credit card and bank statements for any errors or unauthorized transactions promptly and thoroughly.
      - Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
      - Immediately notify the BSI if there are unauthorized entries or transactions in the account.

   d) Check for the right and secure website.
      - Before doing any online transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.
      - Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with *"https"* and a closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display a security certificate information of the site.
      - Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink to it from a website that may not be as secure.
      - If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online.

   e) Protect personal computer from hackers, viruses and malicious programs.
      - Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
      - Ensure that the anti-virus program is updated and runs at all times.
      - Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.

- Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.
- Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online.
- Never download any file or software from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus that could hijack personal information, including password or PIN.

f) Do not leave computer unattended when logged-in.
- Log-off from the internet banking site when computer is unattended, even if it is for a short while.
- Always remember to log-off when e-banking transactions have been completed.
- Clear the *memory cache* and *transaction history* after logging out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.

g) Check the site's privacy policy and disclosures.
- Read and understand website disclosures specifically on refund, shipping, account debit/credit policies and other terms and conditions.
- Before providing any personal financial information to a website, determine how the information will be used or shared with others.
- Check the site's statements about the security provided for the information divulged.
- Some websites' disclosures are easier to find than others — look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a site. If the customer is not comfortable with the policy, consider doing business elsewhere.

h) Other internet security measures:
- Do not send any personal information particularly password or PIN via ordinary e-mail.
- Do no open other browser windows while doing online transactions.
- Avoid using shared or public personal computers in conducting financial transactions.
- Disable the "file and printer sharing" feature on the operating system if conducting financial transactions online.
- Contact the concerned BSI to discuss security concerns and remedies to any online e-services account issues.

2. Other Electronic Products/Channels

a) Automated Teller Machine (ATM) and debit cards
- Use ATMs that are familiar or that are in well-lit locations where one feels comfortable. If the machine is poorly lit or is in a hidden area, use another ATM.
- Have card ready before approaching the ATM. Avoid having to go through the wallet or purse to find the card.
- Do not use ATMs that appear to have been tampered with or otherwise altered. Report such condition to the BSI.

- Memorize ATM personal identification number (PIN) and never disclose it with anyone. Do not keep those numbers or passwords in the wallet or purse. Never write them on the cards themselves. And avoid using easily available personal information like a birthday, nickname, mother's maiden name or consecutive numbers.
- Be mindful of "shoulder surfers" when using ATMs. Stand close to the ATM and shield the keypad with hand when keying in the PIN and transaction amount.
- If the ATM is not working correctly, cancel the transaction and use a different ATM. If possible, report the problem to the BSI.
- Carefully secure card and cash in the wallet, handbag, or pocket before leaving the ATM.
- Do not leave the receipt behind. Compare ATM receipts to monthly statement. It is the best way to guard against fraud and it makes record-keeping easier.
- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the BSI.

b) Credit cards

- Never disclose credit card information to anyone. The fraudulent use of credit cards is not limited to the loss or theft of actual credit cards. A capable criminal only needs to know the credit card number to fraudulently make numerous charges against the account.
- Endorse or sign all credit cards as soon as they are received from the BSI.
- Like ATM card PINs, secure credit card PINs. Do not keep those numbers or passwords in the wallet or purse and never write them on the cards themselves.
- Photocopy both the front and back of all credit cards and keep the copies in a safe and secure location. This will facilitate in the immediate cancellation of the card if lost or stolen.
- Carry only the minimum number of credit cards actually needed and never leave them unattended.
- Never allow credit card to use as reference (credit card number) or as an identification card.
- Never give your credit card account number over the telephone unless dealing with a reputable company or institution.
- When using credit cards, keep a constant eye on the card and the one handling it. Be aware of the "swipe and theft" scam using card skimmers. A skimmer is a machine that records the information from the magnetic stripe on a credit card to be downloaded onto a personal computer later. The card can be swiped on a skimmer by a dishonest person and that data can then be used to make duplicate copies of the credit card.
- Do not leave documents like bills, bank and credit card statements in an unsecure place since these documents have direct access to credit card and/or deposit account information. Consider shredding sensitive documents rather than simply throwing them away. (Some people will go through the garbage to find this information).
- Notify the BSI in advance of a change in address.
- Open billing statements promptly and reconcile card amounts each month.

- Do not let other people use your card. If card is lost or stolen, report the incident immediately to the BSI.

c) Mobile Phones/Devices
   - Do not disclose your Mobile Banking Pin (MPIN) to anyone.
   - Regularly change the MPIN.
   - Do not let other people use your mobile phone enrolled in a mobile banking service. If the phone is lost or stolen, report the incident immediately to the BSI.
   - Be vigilant. Refrain from doing mobile banking transactions in a place where you observe the presence of "shoulder surfers".
   - Keep a copy of the transaction reference number provided by the Bank whenever you perform a mobile banking transaction as an evidence that the specific transaction was actually executed.

Since customers may find it difficult to take in lengthy and complex advice, BSIs should devise effective methods and channels for communicating with them on security precautions. They may make use of multiple channels (e.g. BSI websites, alert messages on customers mobile phone, messages printed on customer statements, promotional leaflets, circumstances when BSI's frontline staff communicate with their customers) to enforce these precautionary measures.