IT RISK MANAGEMENT STANDARDS AND GUIDELINES
Area: Information Security
(*Appendix to Sec. 148 on Purpose and Scope, and IT Risk Management Systems, and Sec. 149 on Other Policies, Standards and Processes*)

1. INTRODUCTION

1.1 Information, as one of the most critical assets of Bangko Sentral Supervised Financial Institutions (BSFIs), should be accorded with adequate level of protection and risk management controls to preserve its confidentiality, integrity, and availability. BSFIs are increasingly relying on information to achieve business goals and objectives, drive core operations, and support critical decisions. With the emergence of new business models in a predominantly information-driven economy, information that is timely, accurate, and reliable becomes even more important. Effectively addressing information security requirements enables BSFIs to remain competitive and relevant as the financial services industry moves towards digital innovation. Thus, BSFIs need to prioritize information security risk management (ISRM) aligned with their business goals and objectives.

1.2 Information security instills trust and confidence between BSFIs and their customers, ensures compliance with laws and regulations, and improves enterprise value. Because information security is intrinsically linked to the overall safety and soundness of BSFIs, the Board of Directors (Board) and Senior Management should exercise effective information security governance to ensure ongoing alignment of information security with business needs and requirements. Information security risks and exposures must be managed to within acceptable levels through a dynamic interplay of people, policies and processes, and technologies and must be integrated with the enterprise-wide risk management system.

1.3. The frequency, severity, and visibility of recent cyber-attacks highlight, not only the degree of disruption to business operations, but also the extent of reputational damage which could undermine public trust and confidence in the financial system. If not properly managed, cyber-attacks may result to operational, legal, reputational, and systemic risks. In light of the growing concerns on cybersecurity, a key component of information security, BSFIs should put greater emphasis on cybersecurity controls and measures in managing information security risks.

2. INFORMATION SECURITY GOVERNANCE

2.1. **Information Security Strategic Plan.** An information security strategic plan (ISSP), aligned with the BSFI’s business plan, must be established to clearly articulate the Board and Senior

Management's direction on information security. The ISSP should provide a roadmap that would guide the BSFI in transforming the current state of security to the desired state taking into account business goals and strategies. In defining the desired state of security, the concerned BSFI should consider key elements, to include principles and policy framework, organizational structures and culture, information/data, services, IT infrastructure, and people.

The BSFI may utilize commonly accepted approaches or frameworks in developing the ISSP tailored to its specific business and technology profile. The ISSP must be reviewed at least annually by the Board and Senior Management and regularly updated in line with changes in business strategies, IT infrastructure and services, and operating environment.

2.2. Information Security Program. The BSFI should maintain a comprehensive, well designed and effective Information Security Program (ISP) commensurate with its operational and IT profile complexity. The ISP is essentially the mechanism to implement the ISSP which must be aligned with business needs and strategies and integrated across all facets of the business environment. To ensure its effectiveness and sustainability, the ISP should have strong support from the Board and Senior Management as well as cooperation of all concerned stakeholders. The program should clearly establish security roles, responsibilities and accountabilities, and provide mechanisms to ensure enforcement and compliance (e.g. formal disciplinary process and corresponding actions for those who have committed security violations). The ISP generally covers security policies, standards and procedures, security operations, technologies, and organizational structures as well as security awareness and training programs aimed at protecting BSFI's information assets and supporting infrastructure from internal and external threats.

The ISP should be reviewed and tested at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. Management should adjust the ISP to reflect the results of ongoing risk assessment, analyses of emerging internal and external threats and vulnerabilities, cyber-intelligence gathered from information sharing groups, and the level of effectiveness of the existing security controls. Further, Management should take into account changes in the IT infrastructure/systems and business arrangements such as mergers, acquisitions, alliances and joint ventures, and outsourcing agreements.

2.3 **Security Culture.** The Board and Senior Management should take the lead in establishing an information security culture that regards security as an intrinsic part of the BSFI's core business and operations. Instilling a strong security culture ensures that security controls, processes and measures are deeply embedded into the BSFI's lines of business, products, services and processes, including its employees and external relationships. Having a strong security culture will help facilitate attainment of the institution's desired state of security and level of maturity

as well as more effective and efficient implementation of the ISSP and ISP. The level of compliance of employees to the security policies, employees' knowledge in identifying and reporting incidents, and the degree of integration of security requirements throughout the life cycles of services and applications are some indicators of an institution's security culture. The Board and Senior Management should adopt the right mindset and understand the crucial role of information security in supporting/achieving business goals and objectives. In line with this, the Board and Senior Management should provide the necessary resources to develop, maintain, and implement the ISP.

2.4 **Responsibility and Accountability.** Information security roles and responsibilities span the entire organization from the Board and Senior Management, business line managers, security department, down to the employees. The BSFI's Board and Senior Management set the overall tone and strategic direction for information security by providing strong leadership and effective information security governance. The Board, or an appropriate Board committee, is responsible for overseeing the development, implementation and maintenance of the BSFI's ISSP and ISP. The Board should understand the business case for information security as well as the impact of information security risks to the business. Relative thereto, the Board should approve and provide adequate funding and other necessary resources for security projects and initiatives to effectively implement the ISSP and ISP. The Board or a Board-designated committee should approve and review the written ISSP and ISP including the corresponding security policies and standards at least annually. The Board or a Board-designated committee should likewise periodically review the assessments of the overall effectiveness of the program and direct Senior Management to undertake corrective actions, when necessary.

Senior Management is generally responsible and accountable in executing the ISSP and ISP within the bounds and thresholds set by the Board. Senior Management plays a key role in providing leadership and support for information security as well as balancing business and security requirements and managing information security risks within acceptable levels. Senior Management should appoint a Chief Information Security Officer (CISO) who will be responsible and accountable for the organization-wide ISP. The duly appointed CISO is a senior level executive with sufficient authority within the institution to effectively perform the following functions and responsibilities, among others:

a. Formulate the ISSP and ISP for approval by the Board and Senior Management;
b. Implement and manage the duly-approved ISSP and ISP;
c. Coordinate and work with business process owners and executives across different departments to ensure that information security requirements support business needs and security systems and processes are working as intended;
d. Enforce compliance with the ISP and the corresponding policies, standards and procedures

across the organization and conduct security awareness and training programs catered to different sets of stakeholders;

e. Educate, inform, and report to the Board and Senior Management relevant information security issues and concerns;
f. Prepare business cases for certain security control technologies, products, and arrangements for Board and Senior Management's approval;
g. Ensure that security controls and processes are embedded throughout the lifecycle of information, systems, applications, products and services;
h. Assist in the effective implementation of information security incident response plan; and
i. Assist in ensuring regulatory compliance and adherence to information security-related laws, rules and regulations.

In addition to the minimum qualifications provided in Sec. 134, the appointed CISO should have sufficient knowledge, technical background, skills and training to enable him to perform the above assigned tasks. To ensure appropriate segregation of duties, the CISO should report directly to the Board, designated Board committee or to Senior Management and have sufficient independence to perform his mandate. The CISO should perform the tasks of a risk manager and should be independent from the IT department. For BSFIs with moderate to complex IT profile classification, the CISO may be the head of an information security office/unit, staffed with a number of highly skilled security specialists. In the case of BSFIs with simple IT profile, the CISO function may be assigned to an existing independent officer who meets the above qualifications.

The BSFI's IT department also plays a crucial role in maintaining security within the technology domain. Considering that security controls and measures are largely automated and technology-driven, it may be more feasible for BSFI's security operations personnel and IT personnel to share some security administration functions. IT personnel are usually charged in managing the security configuration of servers, databases, routers, switches and other security technologies that are deeply embedded in systems/applications.

Security specialists, on the other hand, are responsible in managing the more specialized security tools and technologies such as Security Information and Event Management (SIEM) tools, vulnerability scanners, and other management support technologies.

Insofar as the ISP includes physical security as one of the IS controls, the CISO may need to coordinate with the BSFI's Chief Security Officer or Bank Security Officer on IS matters/incidents that entail physical security considerations. The CISO should also collaborate with fraud management units (FMU), particularly in monitoring emerging security and fraud risks involving customer accounts.

Business line managers, application/system and information owners are generally responsible for information asset classification and determining the required level of security requirements to support business requirements. They are also responsible in defining and granting access rights of employees and ongoing monitoring of the appropriateness of such access rights. On the other hand, employees, as the first line of defense, should understand and abide by the security policies, standards and procedures. They are responsible in monitoring and reporting security-related incidents and security lapses within their job functions in accordance with the information security incident response plans. To ensure their ongoing commitment and awareness, employees should regularly attend security awareness trainings and other programs.

2.5. **Resources.** The Board and Senior Management should see to it that adequate resources, organizational functions/capabilities, policies, standards and procedures as well as the supporting infrastructure commensurate with the BSFI's IT profile classification and risk appetite, are available and optimized to effectively implement the institution's ISSP and ISP. Without sufficient resources in terms of funding/budget allocations, skilled manpower and underlying technologies, implementation of the ISP may suffer leading to security lapses, incidents and poorly designed/implemented security systems. Thus, it is crucial that sufficient resources are devoted to information security operations and initiatives. Further, Management may supplement its existing security skills and capabilities through outsourcing of certain security functions to third party service providers, including cloud service providers. In such cases, the institution needs to provide adequate oversight and institute robust risk management processes and practices pursuant to existing regulations on outsourcing and cloud computing.

2.6. **Compliance with Relevant Laws, Regulations and Standards.** In designing the ISSP and ISP, compliance with relevant laws, regulations, and standards must be fully considered. For BSFIs, these include The Law on Secrecy of Bank Deposits under R.A. No. 1405 and recently, the Data Privacy Act of 2012 under R.A. No. 10173. For BSFIs that process and issue payment cards under international brand schemes (e.g., VISA, Mastercard, AMEX, etc.), the ISP should be tailored to fit the requirements of the Payment Card Industry Data Security Standard (PCI DSS). Moreover, Management may find having security certifications such as those provided by the International Organization for Standardization (ISO) and other certifying bodies to be of significant value to the business.

These certifications serve as proof of certain quality and standards in terms of information security management systems which may enhance customers' and stakeholders' confidence, facilitate regulatory compliance on security, and enable achievement of desired security posture and maturity. While not specifically required under the Bangko Sentral regulations,

obtaining security certifications may be considered a sound security practice that may speed up the maturity level of the BSFI and a sound indicator of effective information security culture. Management should continually assess the regulatory environment and adjust/update their ISSP and ISP accordingly to ensure continuing compliance.

3. ISP MANAGEMENT

3.1. **Information Security Risk Management System.** The Information Security Risk Management (ISRM) system should be an integral part of the organization's ISP and enterprise-wide risk management system. The ISRM framework, including cybersecurity elements, should be commensurate to the level of risk profile of the BSFI. The design and implementation of the ISRM system largely depends on the BSFI's culture, mission and objectives, organizational structure, products, services, and management/operational processes. To ensure that appropriate information security controls and maturity levels are achieved, Management may refer to leading standards and technology frameworks[1] in designing the institution's own ISRM framework.

3.1.1. **Risk Management Process.**

Management should conduct periodic security risk assessment to identify and understand risk on confidentiality, integrity and availability of information and IT systems based on current and detailed knowledge on BSFI's operating and business environment. This includes identifying information security risks relative to its internal networks, hardware, software, applications, systems interfaces, operations and human elements. The risk assessment should include an identification of information and IT resources to be protected and their potential threats and vulnerabilities. This risk identification phase should be comprehensive to cover all possible risk scenarios that may hamper the confidentiality, integrity and availability of information assets.

An effective risk assessment process involves three phases namely: risk identification, analysis and evaluation. Vendor concerns place additional elements to the process. The risk identification process, including the elements that the BSFI needs to consider is further detailed in item 3.2 Identification phase.

Once the risks are identified, Management should undertake a systematic risk analysis phase whereby the likelihood and impact of threats and vulnerabilities are assessed. It should utilize clearly defined and consistent risk measurement approaches in analyzing and evaluating risks. After which, the appropriate risk treatment options (i.e., mitigate, transfer, avoid or accept) should be applied taking into consideration the

BSFI's risk appetite and tolerance. Once the BSFI identifies the risks to mitigate, Management can begin to develop risk mitigation strategy which should be an integral component of the ISP. The risk management phases from identification to risk treatment should flow into the BSFI's risk reporting and monitoring activities to ensure effectiveness and continuous improvement of the entire risk management process. The results of the risk management processes should be communicated to the concerned stakeholders and reported to the Board and Senior Management for appropriate risk decisions.

3.1.1.1. **Insurance.** The BSFI may avail of insurance coverage for information security related events and incidents as a way to transfer risks. It is, however, not to be construed as a substitute for an effective ISP. Insurance is a logical risk treatment option for risk exposures with high impact but with low probabilities (e.g., fire, earthquakes, massive cyber-attacks, etc.). Hence, it should carefully evaluate the extent and availability of coverage in relation to the magnitude and probability of the risks. Likewise, Management should ensure compliance with relevant security controls and policies as stipulated in the insurance policy.

3.2. **Identification.** Management should be able to identify the BSFI's information security as well as cyber-related risks through a thorough understanding of its business processes and functions, information assets and related access, threats and vulnerabilities, interconnections, and security architecture. The identification process is the first crucial step to information security risk management and should be robust enough to ensure that all foreseeable risks and threats are identified. Failure to identify key information security risks would significantly hamper the security posture, as such would no longer be considered in the analysis and mitigation phases.

3.2.1. **Business Processes and Functions.** The BSFI constantly faces the challenge of balancing its security requirements versus performance objectives and costs. Similar to the conduct of business impact analysis (BIA), Management should identify all business processes and functions, including their dependencies and consequently assess and determine their criticality and importance to the business. This exercise should guide the BSFI's decision-makers in prioritizing preventive, detective, response and recovery efforts. The level and degree of security controls and measures are expected to be commensurate to the criticality and importance of the business processes and functions. At a minimum, Management should ensure that the ISP is able to adequately support/secure the institution's critical business processes and functions.

3.2.2. **Information Assets and Related Access.** The BSFI should maintain an inventory of all information systems assets that include components from all information systems. In developing an information systems assets inventory, it should be able to document system-specific information (e.g., hardware inventory specifications, software license information, software version numbers, component owners, machine names, network address, manufacturer, device type, model, serial number, and physical location) that will allow Management to:

a. Identify the information owner who shall be responsible in ensuring confidentiality, integrity, and protection of these assets;
b. Associate the interdependencies of these systems and understand how these systems support the associated business lines;
c. Facilitate an efficient process for system installations, removals, and other updates; and
d. Monitor system configuration activities and detect unauthorized changes to the systems in a timely manner.

3.2.3. **Threats and Vulnerabilities.** In identifying risks, the BSFI should have a documented process that will determine the threats and vulnerabilities to the institution's IT environment. A threat is anything or anyone that has the potential to adversely impact the institution by exploiting vulnerability in people, process, and/or technology. Given the broad definition of threat, the BSFI should establish a structured approach that will allow Management to have a holistic view of the threat landscape. This can be done by maintaining robust threat intelligence feeds from various sources such as publicly available data from news media, publications and websites as well as subscription to information security vendors and information-sharing organizations.

Threat identification and management programs should enable the BSFI to:
a. Identify and understand the nature, frequency, and sophistication of threats;
b. Categorize threats, sources, and vulnerabilities;
c. Aggregate and quantify potential threats;
d. Evaluate the corresponding information security risks to the institution; and
e. Develop appropriate risk mitigation strategies as part of the ISP.

As threats continue to evolve rapidly and increase in sophistication, Management should ensure that threat monitoring and vulnerability scanning tools and processes remain effective in identifying both known and unknown (zero-day[2]) security exposures.

3.2.4. **Interconnections.** The BSFI's business processes often deal with exchanging

information and conducting transactions in an online and interconnected environment which inevitably require third-party connections to its network and computing resources and vice versa. These arrangements should be governed by terms and conditions that clearly establish the duties and responsibilities of both parties in owning, operating, and/or maintaining the information systems. The extent of interconnection may result to risks that may weaken the institution's security posture.

As such, it should identify connections with external parties, including other BSFIs, financial market infrastructures and third party service providers, their corresponding access points and channels and systems/applications accessed. Consequently, Management should assess the BSFI's interconnectivity risks and implement appropriate risk mitigation controls to improve resilience of the entire ecosystem.

3.2.5. **Security Architecture.** Given the increasing interconnectivity and complexity of information systems and security infrastructure, developing an information security architecture using generally acceptable architectural approaches can provide the BSFI with a holistic view of existing security controls and processes, the taxonomy of business processes and information and information flows and their interdependencies. For complex BSFIs, an information security architecture that is aligned with their enterprise architecture should be adequately documented. The development of the information security architecture should also incorporate security controls needed to support data privacy requirements. The information security architecture generally includes an architectural description, placement of security controls, security-related information for external interfaces, information being exchanged across the interfaces, and protection mechanisms associated with each interface.

3.3. **Prevention.** Management should put in place adequate protection mechanisms and controls to prevent security incidents and risks from materializing. These include measures ranging from baseline to advanced tools and approaches such as defense-indepth, malware prevention, access controls, and cybersecurity awareness programs, among others. These preventive controls are generally categorized into three types, namely: administrative, physical and environmental, and technical controls.

3.3.1. **Administrative Controls.** The BSFI should establish administrative controls to clearly articulate the Board and Senior Management's intent, expectations, and direction on information security. Administrative controls generally address the human factor affecting information security within all levels of the organization.

3.3.1.1. **Policies, Standards, and Procedures.** Management should formulate written

information security policies, standards, and procedures which define the institution's control environment and guide employees on the required, expected, and prohibited activities. Policies, standards, and procedures serve as a primary tool in the exercise of effective information security governance, hence, they should be able to capture the Board and Senior Management's security direction and risk appetite. The Board and Senior Management should approve and periodically review policies, standards, and procedures to ensure ongoing alignment with business needs and requirements. Policies, standards, and procedures should have the following attributes:

a. Documented using clear, simple, and unambiguous language and widely communicated to all employees and concerned stakeholders;

b. Comprehensive and complete covering all aspects of ISRM such as, but not limited to, security organizational structure, physical, environmental and logical security, communications and operations management, and human resources security;

c. Tailored to the needs and requirements, including the security culture of the institution; and

d. Adaptable to the changing business, regulatory, and operating environment.

3.3.1.1.1. **Minimum Baseline Security Standards.** Management should put in place minimum baseline security standards (MBSS) to ensure that systems, hardware, and network devices are consistently and securely configured across the organization. These standards enable the deployment of operating systems, databases, network devices, and mobile devices within the IT environment in an efficient and standardized manner. Management may refer to leading standards and best practices as well as vendor-specific recommendations in developing their MBSS, taking into consideration the following controls:

a. Secure configuration of operating systems, system software, databases, and servers to meet the intended uses with all unnecessary services and programs disabled or removed;

b. Periodic checking to ensure that baseline standards are

consistently complied with;

c. Timely deployment of tested and approved patches and security updates;

d. Adequate documentation of all configurations and settings of operating systems, system software, databases, and servers; and

e. Adequate logging capabilities for all systems, applications, network devices, and databases.

3.3.1.2. **Security Training and Awareness Programs.** All employees of the organization and, where relevant, contractors and third party users should receive appropriate information security awareness training and regular updates in organizational policies and procedures relevant to their job function. Awareness and education are vital components in the overall security strategy of the BSFI as they address the weakest link in the security chain. Security training and awareness programs promote a security conscious environment and strengthen compliance with the BSFI's security policies, standards, and procedures.

Security training and awareness programs should be designed and tailored to the specific requirements of different groups and stakeholders (i.e., business process/information owners, security specialists, incident responders, etc.). The program should be constantly updated to cover emerging threats and risks and must include defined metrics to enable the BSFI to assess its effectiveness over time.

3.3.1.3. **Security Screening in Hiring Practices.** Management should have a process to verify job application information of all new employees. Screening procedures, including verification and background checks, should be developed for recruitment of permanent and temporary IT staff, and contractors, particularly for sensitive IT-related jobs or access level. Similar checks should be conducted for all staff, including contractors, at regular intervals throughout their employment, commensurate with the nature and sensitivity of their job functions as well as their access to critical systems. Management should be aware of changing personal circumstances of employees and contractors that may be indicative of potential increased incentives for system misuse or fraud. Further, it should establish processes and controls to mitigate risks related to

employees' termination/resignation or changing responsibilities.

3.3.1.4. **Security Screening in Hiring Practices.** Management should have a process to verify job application information of all new employees. Screening procedures, including verification and background checks, should be developed for recruitment of permanent and temporary IT staff, and contractors, particularly for sensitive IT-related jobs or access level. Similar checks should be conducted for all staff, including contractors, at regular intervals throughout their employment, commensurate with the nature and sensitivity of their job functions as well as their access to critical systems. Management should be aware of changing personal circumstances of employees and contractors that may be indicative of potential increased incentives for system misuse or fraud. Further, it should establish processes and controls to mitigate risks related to employees' termination/resignation or changing responsibilities.

3.3.2. **Physical and Environmental Controls.** Physical security measures should be in place to protect computer facilities and equipment from damage or unauthorized access that can impair the confidentiality, integrity, and availability of information. 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 upon presentation of proper identification and authentication process (i.e., ID cards, badges, biometrics, etc.). Moreover, a specific and formal authorization process should be employed for the removal of hardware and software from the premises.

Since the data center houses the BSFI's most critical information processing facilities, Management should fully consider the environmental threats (e.g., proximity to dangerous environment hazards) when selecting sites for data centers. Buildings should give minimum indication of their purpose, with no obvious signs identifying the presence of information processing facilities. Moreover, physical and environmental controls should be implemented to prevent, detect, and 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 backup generators. Management should ensure that these systems and devices regularly undergo preventive maintenance to ensure that they are in good working condition and operating as intended.

3.3.3. **Technical Controls.** Management should employ robust and multi-layered technical controls to ensure that the confidentiality, integrity, and availability objectives for information assets are met. These consist of various logical security controls, security tools, and technologies which provide defense against system compromise. Technical controls represent the technology factor in information security that should be working in tandem with the BSFI's policies, standards, and processes.

3.3.3.1. **Technology Design.** Management should consider information security and cyber resilience during the infrastructure build-up, systems development and product design. It should ensure that applicable standards and operating procedures are in place for all software, network configurations, and hardware connected to critical systems. Management should also understand the benefits and limitations of the technology that the institution uses and provide compensating controls when necessary. Management should also adopt mechanisms to continually assess whether processes, people, and technologies support the desired level of information security based on the BSFI's size, complexity, and risk profile.

3.3.3.2. **Identity and Access Management.** The BSFI should adopt a sound and systematic identity and access management program following the principles of least privilege and segregation of duties. Access rights and system privileges granted should be the minimum required for users to perform their job functions and responsibilities. No person, by virtue of rank or position, should have unrestricted and unauthorized access to confidential data, applications, system resources or facilities.

The BSFI should have an effective process to manage user authentication and access control consistent with the criticality and sensitivity of the information/system. The grant, modification, and removal of user access rights should be approved by the information/system owner prior to implementation. Information/system owners or business line managers should ensure that user access rights remain appropriate through a periodic user access re-certification process. Obsolete user accounts or inappropriate access rights should be disabled/removed from the systems in a timely manner.

Prior to granting access to systems, users should be required to sign an acceptable-use policy (AUP) to promote user awareness and accountability in conforming to security policies and procedures. The BSFI should have password standards in place to ensure that user passwords are not easily compromised

(i.e., password syntax, validity, system-enforced password changes). Stronger authentication methods, such as the use of multi-factor authentication techniques, should be deployed for high-risk transactions (e.g., large value funds/wire transfers, enrollment of billers, systems administration functions).

Default user accounts defined in new software and hardware should either be disabled or changed and subject to close monitoring. Privileged access and use of emergency IDs should be tightly controlled as it gives the user the ability to override system or application controls. The necessary controls include:

a. Formal approval process on a need-to-use or event-by-event basis;

b. Prohibiting shared usage of privileged accounts/IDs;

c. Logging and monitoring of activities performed;

d. Proper safeguard of privileged and emergency IDs and passwords (e.g., kept in a sealed envelope and locked in a secure place inside the data center); and

e. Change of privileged and emergency IDs' passwords immediately upon return by the requesters.

3.3.3.2.1. **Remote Access.** The BSFI, in line with business strategies and needs, may allow employees to connect remotely to the institution's network using either an institution-owned or a personally owned device (often referred to as "bring your own device" or BYOD). Management should ensure that such remote access is provided in a safe, secure, and sound manner to manage attendant risks. At a minimum, the BSFI should establish control procedures covering:

a. Formal authorization process for granting remote access;

b. Risk-based authentication controls for remote access to networks, host data and/or systems, depending on the criticality and sensitivity of information/systems;

c. Securing communication channels, access devices and equipment

from theft, malware and other threats (i.e., encryption, strong authentication methods, data wipe capabilities, application whitelisting[3]); and

d. Logging and monitoring all remote access communications.

For BYOD, Management should fully understand the benefits in line with business goals/strategies as well as the risks in adopting BYOD policy. An effective mechanism should be in place to ensure that personal devices meet certain security standards, such as operating system version, patch levels, and anti-malware solutions, before these can be allowed to access the internal network.

3.3.3.3. Network Security. Management should adopt robust and multi-layered controls to prevent and detect unauthorized access, misuse, and other threats from entering and/or spreading into its internal computer networks and systems. Effective controls should be employed to adequately secure system and data within the network which include the following, among others:

a. Grouping of network servers, applications, data, and users into security domains or zones (e.g., untrusted external networks, external service providers, or trusted internal networks);
b. Adopting security policies for each domain in accordance with the risks, sensitivity of data, user roles, and appropriate access to application systems;
c. Establishment of appropriate access requirements within and between each security domain;
d. Implementation of appropriate technological controls to meet access requirements consistently;
e. Monitoring of cross-domain access for security policy violations and anomalous activity; and
f. Maintaining accurate network diagrams and data flow charts[4].

Commonly used tools and technologies to secure the network include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and demilitarized zones, among others. As the network complexity as well as threats affecting the network evolve, the BSFI should continuously monitor and enhance its network security and systems to ensure that they remain secure, safe, and resilient.

Additional controls should be adopted for Wireless Local Area Networks (WLAN) implementations since these are inherently less secure than wired networks. Controls such as limiting of WLAN signals to authorized areas, physically securing wireless access points and formally approving installations of wireless devices/gateways and active monitoring of the WLAN environment should be employed on top of the usual network security controls. Management may also consider implementing network access control (NAC) systems to prevent recognition and connection of unauthorized or rogue devices into the network.

3.3.3.3.1. **Virtualization.** As BSFis are increasingly leveraging on virtualization technologies to optimize existing hardware resources, reduce operating expenses and improve IT flexibility and agility to support business needs, additional security risks such as attacks on hypervisor integrity and lack of visibility over intra-host communications and virtual machine (VM) migrations are also rising. To address such risks, Management should extend security policies and standards to apply to virtualized servers and environment. Likewise, it should adopt the following control measures:

a. Hypervisor hardening with strict access controls and patch management;

b. Inspection of intra-host communications {traffic within VM environments) and ensuring that security control measures are implemented for confidential/sensitive data stored in VMs; and

c. VM creation, provisioning, migration, and changes should undergo proper change management procedures and approval processes similar to deployment of physical network/system devices and servers.

The BSFI may also consider implementing next generation firewalls that can restrict access more granularly and prevent virtualization-targeted attacks that exploit known VM vulnerabilities and exploits.

3.3.3.4. **Application Security.** Management should ensure that all applications, whether developed in-house or acquired off-the-shelf, have appropriate controls

commensurate to the sensitivity and criticality of applications. Core banking applications as well as other applications considered as mission-critical (e.g., loans, general ledger and treasury systems) should have embedded security control features to maintain information confidentiality, integrity and availability. Secure coding practices which consider security control requirements early into the development phase should be incorporated in the BSFI's application systems development and acquisition policies and procedures. New applications, including subsequent enhancements, should be adequately tested using various testing methodologies (e.g., penetration tests, vulnerability assessments, and application security tests) before loading into production. In case third parties were engaged to develop the applications, Management should exercise adequate oversight to ensure that the level of risk management and security controls/standards is consistently applied.

Security controls within applications should have adequate access and authentication controls, audit trails and logs, and logical controls appropriate to the applications' business purpose and function (e.g., maker/checker functionalities, transaction limits and alerts). Application systems reviews, penetration testing and vulnerability assessments should be periodically conducted to ensure that the applications meet the desired level of security.

3.3.3.5. **Data Security.** The BSFI should have information classification strategy guidelines and institute appropriate set of controls and procedures for information protection in accordance with the classification scheme. Information should be protected throughout its life cycle from handling, storage or data-at rest, transmission or data-in-transit, up to the disposal phase.

3.3.3.5.1. **Data-at-Rest.** Policies, standards, and procedures as well as risk management controls must be in place to secure the BSFI's information assets, whether stored on computer systems, physical media, or in hard copy documents. The level of protective controls shall depend on the sensitivity and criticality of the information. Sensitive information such as system documentation, application source code, and production transaction data are expected to have more extensive controls to guard against alteration or data leakage (e.g., integrity checkers, cryptographic hashes, data leakage prevention systems). Management should likewise implement appropriate controls over information stored on portable devices such as laptops, smart phones, and tablets taking into account their

susceptibility to lost or theft. Applicable risk mitigation controls include data encryption, host-provided access controls, homing beacons, and remote wiping or deletion capabilities, among others.

Considering the unique risk dimensions of storing data in cloud computing platforms, Management should fully understand the nature of the cloud technology in line with business requirements and satisfy themselves as to the level of security (e.g., how access is controlled and how information is retrieved) and compliance to data privacy and other relevant rules and regulations. Information security and accountability still rests with the institution's Management, hence, it should exercise effective oversight over the cloud service provider in terms of adherence to security, performance and uptime, and back-up and recovery arrangements contained in the contract/agreement.

3.3.3.5.1.1. **Database security.** The BSFI should adopt policies, standards, and procedures to adequately secure databases from unauthorized access, misuse, alteration, leakage and/or tampering. Considering their criticality, sensitivity and business impact, access authorizations to databases should be tightly controlled and monitored. Databases should be configured properly and securely with effective preventive and detective controls such as encryption, integrity checkers, logs and audit trails, among others.

3.3.3.5.1.2. **Data-in-transit.** Data transfers are commonly done through physical media or electronic transmission. Policies, standards, and procedures should be in place for maintaining the security of physical media containing sensitive information while in transit, including to off-site storage, or when shared with third parties. These include contractual requirements incorporating risk-based controls, accreditation process for carriers/couriers, packaging standards, encryption of sensitive information, tracking of shipments, and non-disclosure agreements, among others.

Electronic transmission may be done using various channels such as e-mail, file transfer protocols, secure shell, dedicated line, short message service, and the internet. Management should develop policies and procedures and implement appropriate safeguards depending on the channel used. When transmitting sensitive information over a public network, the institution may use encryption controls and techniques such as secure e-mail protocols, secure file transfer protocol (SFTP), and secure socket layer (SSL) certificates to protect against interception or eavesdropping.

3.3.3.5.2. **Removal, Transfers and Disposition of Assets.** Procedures for the destruction and disposal of media containing sensitive information should be risk-based relative to the sensitivity of the information and the type of media used to store the information. Disposal techniques that the BSFI may implement include deletion, overwriting, degaussing[5], destruction of the media. Management should be mindful about residual data being stored in computer-based media as well as dumpster-diving attacks in paper-based information in deciding the best disposal strategy for sensitive information assets. BSFIs should consider applicable Bangko Sentral regulations as well as laws, rules and regulations in developing policies and procedures on disposal of records/media.

3.3.3.6. Malware Protection. Malware threats continue to be a serious concern given their rapid proliferation and advanced capabilities to disrupt operations, corrupt data, and conduct unauthorized transactions. Zero-day exploits and other advanced malwares have the ability to penetrate various access points within the BSFI's network and evade traditional signature-based anti-malware systems and network monitoring controls. To mitigate such risks and ensure resilience against malware threats, Management should adopt layered and integrated anti-malware strategy, including data integrity checks, anomaly detection, system behavior monitoring, and enhanced employee security awareness training programs.

At a minimum, Management should apply the "Least Privilege" principle in granting access to all systems and services and mandate safe computing

practices for all users. Other preventive measures include installation and timely update of anti-malware software provided by reputable vendors, periodic vulnerability scanning, and effective patch management procedures for all critical systems and applications. To address the more sophisticated forms of malware, Management should consider adopting advanced security solutions such as signature-less antimalware solutions capable of analyzing abnormal behavioral patterns in network and system traffic flows. Likewise, application whitelisting which allows only specified programs to run and/or sandboxing technologies which can inspect incoming traffic such as e-mail attachments without compromising the production environment can be employed.

As malware sophistication and capabilities evolve, Management should continuously monitor changes in technologies, threat profiles and the overall operating environment to address emerging risks. It should likewise closely coordinate with its technology vendors and relevant information sharing groups for appropriate remediation procedures.

3.3.3.7. **Encryption.** Encryption, when properly designed, managed, and implemented, can serve as a key control in securing communications, information, and data storage. Management should adopt a sound encryption program covering the following elements:

a. Encryption type, level and strength commensurate to the sensitivity of the information based on the institution's data classification policy;
b. Effective key management policies and practices to properly safeguard the generation, distribution, storage, entry, use, and archiving of cryptographic keys; and
c. Periodic review and testing to ensure that encryption methods deployed still provide the desired level of security vis-a-vis changes in technology and threat landscape.

3.3.3.8. **Integration with IT Processes.**

3.3.3.8.1. Systems Development and Acquisition. Security requirements and considerations should be deeply embedded into the BSFI's systems development and acquisition processes. Involvement of internal audit and information security personnel in the development or acquisition activities should be clearly defined as a means to verify

the adequacy of the control and security requirements as they are developed and implemented.

Aside from 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 clear and specific. The information and/or process owners should check security requirements and conduct user acceptance tests prior to approval of systems to be loaded into the production environment.

Further, BSFIs should maintain separate environments for their development, testing, and production activities respectively. In line with this, programmers/developers should have no access to the production environment. Lastly, strict segregation of duties between developers/programmers and IT operations should be upheld.

3.3.3.8.2. **Change Management.** The BSFI should have an effective and documented process to introduce changes into the IT environment in a safe and secure manner. Such changes should be controlled as to requirements definition, authorization and approvals, testing procedures, and audit trails. Moreover, the process should incorporate review of the impact of changes to the effectiveness of security controls.

3.3.3.8.3. **Patch Management.** Management should adopt a patch management process to promptly identify available security patches to technology and software assets, evaluate criticality and risk of patches, and test and deploy patches within an appropriate timeframe.

3.3.3.8.4. **Vendor Management and Outsourcing.** Management should conduct appropriate due diligence and consider information security in selecting third party service providers (TPSPs). The BSFI should ensure that effective oversight processes are in place to monitor the activities of TPSPs. Contracts should sufficiently detail information security requirements, particularly for TPSPs that store, transmit, process, or dispose of customer information. Mechanisms should be in place to properly monitor the performance of third party service

providers to confirm whether sufficient level of controls is maintained. Considering that TPSPs may be a source of cyber-risks, Management should properly assess cyber-risk exposures from TPSPs in order to proactively adjust their cyber-risk management

3.4. **Detection.** Management should design and implement effective detection controls over the BSFI's networks, critical systems and applications, access points, and confidential information. Detection controls provide the institution with alerts and notifications for any anomalous activities within its network that can potentially impair the confidentiality, integrity, and availability of information assets. Early detection is critical to the BSFI's incident response and recovery procedures as it allows sufficient lead time to institute countermeasures to address impending attacks and contain associated impacts. The detection capabilities are largely a function of people, process, and technology that enable continuous monitoring of the institution's internal networks, systems, applications, and databases.

The level and maturity of the BSFI's detection capabilities should be commensurate to its IT profile classification and operating environment. The selection and design of detection controls largely depends on business priorities and overall security strategy. Detection controls which Management may employ include intrusion detection systems (IDS), virus/malware detection, honeypots, system alerts/notifications, and security incident and event management {SIEM} system. For moderate to complex BSFIs, detection controls are expected to be largely automated to facilitate real-time or near real-time analysis of events such the use of SIEM, IDS, and other technology-based detection systems.

At a minimum, all BSFIs should be able to establish baseline profile of system activity or condition and data flows across the layers of their infrastructure to facilitate monitoring and detection of anomalous activity. Likewise, metrics should be defined for systems, applications and network to determine indicators of possible compromise. For instance, access to a highly-sensitive system beyond office hours or failed log-in attempts of privilege user accounts should prompt real-time or near real-time alerts and notification to concerned security operations personnel.

3.4.1. **Log Management.** Log files can be analyzed for real-time or near real-time detection of anomalous activities, facilitate subsequent investigation of security incidents and can serve as forensic evidence for the prosecution of fraudulent activities. Thus, Management should put in place adequate security controls to prevent unauthorized access, modification and/or deletion of log files. Depending on the criticality of information contained in the log files, Management should implement the following controls to secure the integrity of log files:

a. Encrypting log files containing sensitive data, where feasible;
b. Ensuring adequate storage capacity to avoid gaps in log generation;
c. Restricting access and disallowing modification to log files. Attempts to tamper with log files should prompt activation of system alarms/notifications; and
d. Securing backup and disposal of log files.

3.4.2. **Layered Detection.** In designing the BSFI's detection controls and monitoring capabilities, Management should, to the extent feasible, adopt a layered or defense-in depth approach to ensure that a failure in one control would be compensated by another control. This approach effectively delays or disrupts an attacker's ability to progress within the attack sequence. Tools such as attack trees, event trees, and kill chains may be utilized to enable swift identification and remediation of attacks as they occur.

3.5. **Response.** The response phase is triggered upon confirmation of an occurrence of a cyber-attack or security incident affecting the BSFI and its customers. With the growing incidence of sophisticated cyber-crimes and threats, Management should develop comprehensive, updated, and tested incident response plans supported by well-trained incident responders, investigators, and forensic data collectors. Through adequate response capabilities, Management should be able to minimize and contain the damage and impact arising from security incidents, immediately restore critical systems and services, and facilitate investigation to determine root causes.

3.5.1. **Incident Response Plan and Procedures.** Management should develop and implement a formal incident response plan to address identified information security incidents in a timely manner. The incident response plan should:

a. Provide a roadmap for implementing an incident response process appropriate to the nature, size, and complexity of the institution;
b. Describe the structure and organization that supports the incident response process;
c. Classify incidents, define reportable incidents, and escalation protocols;
d. Define metrics for assessing the incident response process; and
e. Define resources and management support needed to effectively maintain and continuously improve the incident response process.

3.5.2. **Incident Management Process.** Incident handling should follow a well-defined and documented incident management process which sufficiently details the steps from incident analysis and triage assessment, impact mitigation and containment up to testing and continuous improvements.

3.5.2.1. **Incident Analysis and Triage Assessment.** Reported incidents should be investigated to confirm their occurrence and classification. Incidents should be categorized or classified in a manner that enables appropriate prioritization of response and recovery efforts. The category of an incident should guide protocols for communicating to internal and external stakeholders.

3.5.2.2. **Impact Mitigation and Containment.** Upon discovery of an information security incident, the BSFI should seek to contain the damage, mitigate its effects, and eradicate the cause of the incident. Containment measures should be implemented to prevent further harm to the BSFI and/or its customers. Strategies for containment can vary between organizations but typically include the following:

a. Isolation of compromised systems;
b. Remediation and recovery of compromised systems;
c. Collection and preservation of evidence; and
d. Communication with affected parties (e.g., primary regulator, information sharing organizations, law enforcement authorities, customers).

3.5.2.3. **Testing and Continuous Improvement.** Management should define a process for periodically reviewing the incident response plan and updating it based on the BSFI's experience from current and previous incident response activities, including periodic testing exercises.

3.5.3. **Incident Response Teams.** The incident response plan should identify in advance the personnel who will be tasked to respond to an information security incident and clearly define their roles and responsibilities. Organizing a team and assigning responsibilities during an actual incident is likely to cause confusion and may limit the ability of the BSFI to effectively execute response and recovery efforts. In this regard, BSFis should set-up and organize a formal security incident response team (SIRT) tasked to perform, coordinate, and support responses to security incidents and intrusions. Typical SIRT membership includes individuals with varied backgrounds and different areas of expertise including management, legal, public relations, information security, and information technology.

3.5.4. **Crisis Communication and Notification.** The plan should be adequately communicated to appropriate internal and external stakeholders. The BSFI should establish and communicate standard procedures for reporting possible information security incidents to a designated officer or organizational unit.

Concerned BSFIs should promptly notify the Bangko Sentral of any confirmed IT-related fraud cases or major security breaches, pursuant to Sec. 148. Appropriate law enforcement authorities should also be notified in situations involving criminal violations requiring immediate attention. Incidents involving unauthorized disclosure of sensitive personal information should comply with notification rules set by the National Privacy Commission. Customers should also be notified when warranted.

3.5.5. **Forensic Readiness.** Management should implement appropriate controls to facilitate forensic investigation of incidents. Policies on system logging should be established covering the types of logs to be maintained and their retention periods. Applicable Bangko Sentral regulations as well as laws, rules, and regulations on records retention should be complied with. Where a follow-up action against a person or organization after an information security incident involves legal action, evidence shall be collected, preserved, and presented to conform to the relevant rules for evidence.

Management should define in the response plan a systematic process for recording and monitoring information security incidents to facilitate investigation and subsequent analysis. Adequate documentation should be maintained for each incident from identification to closure. Facts about the incident, operational impact, estimated cost, investigation findings, and actions taken by the BSFI should be consistently documented. Automated means of reporting and tracking of incidents may be implemented for analysis and preparation of reports to support decision-making.

3.5.6. **Outsourcing.** For a BSFI without in-house technical expertise, outsourcing of functions related to security incident response including forensic investigations, can be a viable option. In such instances, Management should require the service provider to strictly adhere to the BSFI's policies and standards and ensure confidentiality of data.

3.6. **Recovery.** The recovery phase encompasses both the resumption of activities at a level which is considered "good enough for a certain period of time" and full recovery, i.e., an eventual return to full service. The BSFI should be able to establish back-up facilities and recovery strategies to ensure the continuity of critical operations. During recovery phase, Management should ensure that information processed using back-up facilities and alternate sites still meet acceptable levels of security.

3.6.1. **Business Continuity Management.** Management should develop and implement a formal incident recovery plan to restore capabilities or services that are affected by information security incidents in a timely manner. This can be achieved by incorporating scenarios related to information security (e.g., data breach, malware

outbreak, denial of service) in its business continuity and disaster recovery plans. Refer to Sec. 149 for further guidance on Business Continuity Management (BCM).

3.6.2. **Communication Plan.** A communication plan for information security incidents should be incorporated in the incident recovery plan to facilitate escalation for appropriate management action and to help manage reputation risk. Incidents that lead to publicly visible disruption to BSFI services should be given utmost attention. Timely notification should be given to all relevant internal and external stakeholders (e.g., employees, customers, vendors, regulators, counterparties, and key service providers, media and the public) following a disruption.

Management should consider alternate methods of communication and preparation of predetermined messages tailored to a number of plausible disruption scenarios to ensure various stakeholders are timely, consistently, and effectively informed. Refer to Sec. 149 for further guidance on crisis management.

3.6.3. **Cyber Resilience.** Management should consider the potential impact of evolving cyber events into the BSFI's business continuity planning and institute adequate cyber resilience capabilities. Given the unique characteristics of cyber-threats and attacks, traditional back-up and recovery arrangements adopted may no longer be sufficient. In some instances, it may even exacerbate the damage to BSFI's network, operations, and critical information assets. Hence, Management must consider cyber-related attacks and incidents in the BCM and recovery processes to achieve cyber resilience.

3.6.3.1. **Business Impact Analysis/Risk Assessment.** Management should consider the impact of cyber-threat scenarios during the Business Impact Analysis/Risk Assessment (BIA/RA) phase in conjunction with the ongoing information security risk assessment process. The BSFI should take into consideration a wide-range of cyber-threat scenarios perpetrated from diverse threat sources (e.g., skilled hackers, insiders, state-sponsored groups) which seek to compromise the confidentiality, availability, and integrity of its information assets and networks. Cyber-risks and threats such as malware, distributed denial of service (DDoS) attacks, advance persistent threats (APTs), among others, should be considered in the BIA/RA process.

3.6.3.2. **Defensive Strategies.** Depending on the results of its risk assessments and cybersecurity profile, the BSFI may need to deploy defensive strategies ranging from basic to highly advanced technologies to promote cyber resilience, such as, defense-in-depth or layered controls, reducing attack surfaces, virtual

technologies, air-gap facilities and threat intelligence feeds, among others.

3.6.3.3. **Recovery Arrangements.** Depending on IT and operations risk profile and complexity, Management should consider adopting innovative recovery arrangements that address the unique risks arising from cyber-threats. These include the use of non-similar facility, cloud-based disaster recovery solutions and pre-arranged third party forensic and incident management services.

3.7. **Assurance and Testing.** Management needs to continually assess and test controls and security measures implemented under prevent, detect, respond and recover phases to ensure that these are effective and working as intended. Likewise, a comprehensive, systematic and layered testing and assurance program covering security processes and technologies should be in place. This is to ensure that the ISP is on track in providing appropriate level of information security commensurate to the BSFI's IT profile classification. This phase also ensures that the ISSP and ISP remain effective vis-a-vis the fast-evolving cyber-threat landscape.

3.7.1. **Testing Program.** Given the dynamic nature of information security risks, Management should continually ascertain that the ISP is operating as expected and reaching the intended goals. The scope and depth of testing generally depend on the level of confidence that the Board and Senior Management intend to place on the program. Management should establish a written testing and evaluation plan that assesses the effectiveness of system design and operation, including the integration of security controls, vis-a-vis the level of assurance desired by the Board and Senior Management. At a minimum, the testing plan should have the following key elements:

a. Scope, timing, and frequency of testing;
b. Independence and capability of the testing personnel and review team;
c. Criteria used to ascertain whether the results are acceptable; and
d. Reporting process to the Board and Senior Management.

3.7.2. **Types of Tests and Evaluations.** Considering that no one type of assessment can provide a complete representation of the BSFI's information security posture, Management should employ a variety of effective testing methodologies and practices in order to validate the overall effectiveness of the ISP. Some of the more common types of security assessment/testing with corresponding objectives, brief description and other details, in order of increasing complexity, are as follows:

a. Self-Assessment – an activity conducted by the specific business line or department that typically captures their awareness of the level of risk and effectiveness of

controls concerning their own business processes and functions. Since these are performed by the concerned business units themselves, an independent review process should occur subsequent to the conduct of self-assessment for validation and consistency across the entire BSFI.

b. Security Audit/Review and Compliance Check – is commonly performed by the BSFI's IT auditors, security personnel, and compliance function, respectively, to assess compliance to relevant security policies, standards, and procedures. Internal or external auditors review all aspects of the ISP to determine its overall effectiveness in achieving the desired security results or outcome. Auditors must have the necessary background, training, experience, and independence to effectively discharge their tasks and responsibilities.

c. Vulnerability Assessment (VA} – refers to the identification of security vulnerabilities in systems and network usually through the use of automated vulnerability scanners. Frequency of the performance of vulnerability scans should be determined based on assessment of risk and criticality of systems or information stored on each system. High risk vulnerabilities uncovered during VA exercises should be remediated within a reasonable timeframe.

d. Penetration Testing (PT) – involves subjecting a system or network to simulated or real-world attacks that exploit vulnerabilities under controlled conditions. Depending on the test objectives and scope, the BSFI may use penetration testing to assess potential business impact, the level of security, risk management processes and controls as well as the knowledge of concerned personnel in the organization in identifying, detecting, and responding to attacks.

For BSFIs providing digital/electronic, financial services, VA and PT should be performed by an external party at least annually.

e. Scenario-Based Testing – constitutes a wide range of scenarios, including simulation of extreme but plausible events such as targeted cyber-attacks in testing the BSFI's response, resumption and recovery practices, including governance arrangements and communication plans. To ensure robustness of test scenarios, cyber threat intelligence and threat modeling should be utilized to the extent possible to mimic actual cyber-threats and events.

f. Compromise/Breach Assessment- involves the placement of sensors/tools within the network to actively probe network traffic and system activities to detect, alert, and

potentially mitigate malware intrusions as they occur. This type of assessment addresses advanced malwares and threats with capabilities to evade traditional monitoring systems. Complex BSFIs should conduct regular compromise/breach assessment exercises, on top of other types of tests, to enhance the level of assurance on their security posture as well as their overall situational awareness.

g. Red-Teaming Exercise – a more in-depth type of penetration testing which continually challenges the organization's defenses and controls against cyber attacks. The red team is composed of highly-trained specialists, acting on adversarial mode, which may be the BSFI's own independent employees or third party experts. The end objective is to improve the state of readiness of the entire organization in cases of cyber-attacks.

4. CYBER THREAT INTELLIGENCE AND COLLABORATION

4.1. **Situational Awareness and Threat Monitoring.** In response to rapidly-evolving, sophisticated, and coordinated cyber-attacks targeting financial institutions, BSFIs need to enhance situational awareness as well as their threat monitoring capabilities. Situational awareness is a state whereby the BSFIs' Board and Senior Management are fully aware of the internal and external threat environment as it relates to their IT risk and cyber-risk profiles, operating complexities and business models. Situational awareness entails gathering and maintaining robust threat intelligence about the proficiencies, tactics, and motives of malicious actors/attackers that enable BSFIs to institute appropriate countermeasures quickly. A keen sense of the threat landscape, both from internal and external sources, would greatly help BSFIs in adjusting their ISSP and ISP to achieve cyber resilience. BSFIs should establish a systematic process of gathering, analyzing, and monitoring threat information for actionable intelligence, timely insights, and proactive response. As gathered from Bangko Sentral 's surveillance and monitoring activities, below are some of the top cyber-threats that BSFIs should be wary about with the corresponding prescribed countermeasures/controls:

Threat Description	Prescribed Countermeasures/Controls
Card Skimming – refers to the illegal copying of information from the magnetic stripe of a credit or ATM card to gain access to accounts. This type of fraud usually results to financial losses and unauthorized charges to the customers.	As required under Sec. 148, BSFIs should migrate their entire payment card network to the EMV technology. This is to address the vulnerabilities of magnetic stripe cards from card skimming fraud. Pending full migration to EMV, BSFIs should implement mitigating controls such as those specified under Bangko Sentral Memorandum No. M-2014-040 dated 03 October 2014 on Card Fraud and skimming attacks.

Distributed Denial of Service (DDoS) Attack – makes use of the capacity limitation of enterprise networks, systems or applications with extreme traffic loads or requests that impair their availability to legitimate users.	BSFIs should implement multiple layers of control to prevent, detect, correct, monitor, and analyze system and network anomalies arising from DDoS attacks. These include deployment of on-premise and/or cloud-based solutions, close coordination with internet service providers (ISPs) and hosting companies, as well as having a robust and reliable back-up system. Incident response plans should cover response and recovery procedures for DDoS attacks. In some cases, a DDoS attack is used as a diversionary tactic, hence, BSFIs should be on heightened alert for any signs of infiltration or presence of malware across their IT environment during and after such incident.
Phishing Attacks – involve tricking customers into giving sensitive information through fraudulent emails or websites.	Employee and customer awareness campaigns and education programs are key elements in addressing phishing attacks since these attacks specifically exploit BSFIs' employees, officers and customers. BSFIs should adopt multi-factor authentication for high-risk systems/transactions in order to limit the ability of attackers to consummate the fraud. Further, BSFIs should adopt security measures and mitigating controls prescribed under Memorandum No. M-2015-025 dated 22 June 2015 on Guidance on Management of Risks Associated with Fraudulent E-mails or Websites.
Ransomware and other malwares – refer to malicious software that compromises the confidentiality, availability, and integrity of information systems, networks and data. For ransomware, data or applications are encrypted by the attacker to prevent users from accessing their own data. Only when users pay the "ransom" will these information or systems be released.	On top of the security controls and measures under Item *3.3.3.6* on malware prevention prescribed above, BSFIs, specifically those confronted with ransomware attacks should refrain from paying or communicating with the malicious actor as this does not guarantee that ransomed and/or encrypted files will be released. To mitigate the potential catastrophic impact of ransomware attacks, BSFIs should ensure that adequate back-up and recovery procedures for critical systems and data, including periodic testing to check the integrity thereof, are in place. Because back-ups may also be subject to attacks, BSFIs should consider supplementing existing practices with cloud based back-ups and/or back-ups using removable media or air-gapped facilities.
Advanced Persistent Threats (APT) – are highly-sophisticated attacks which primarily target a specific institution or industry for terrorist aims, corporate espionage or massive fraud schemes. APTs often involve integrity breach wherein core data, systems, and network are compromised and corrupted once an attacker gained foothold and established persistent presence in the target environment.	These types of attacks are generally more destructive compared to the other cyber-threats since the threat actors are highly skilled, motivated, and determined to infiltrate and exploit vulnerabilities on stealth mode. As such, Management should adopt defense-in-depth strategy in preventing and detecting APTs. Likewise, complex BSFIs that are more vulnerable to these types of threats should consider deploying automated and advanced security tools, technologies and methods such as the use of anti-malware solutions, behavior-based fraud management systems and monitoring tools with machine learning capabilities, among others. These technologies should be supported by 24×7 monitoring through a mature SOC. High-risk system should have robust security controls and closely monitored for any anomalous or suspicious activities. A strong security culture should likewise be instilled across the organization as a first line of defense.

4.1.1. **Security Operations Center.** In light of the growing cyber-threat concerns affecting

BSFIs, the need for centralized visibility, continuous monitoring, and rapid response and recovery procedures is increasingly heightened. Hence, centralizing security operations through a security operations center (SOC), equipped with automated security monitoring tools, defined processes and highly-trained personnel, enables BSFIs to keep pace with the tactics of advanced threat actors. Complex BSFIs should put in place an SOC tasked to provide round-the-clock monitoring and real-time analysis of security incidents and cyber-related events.

An SOC is typically organized into three levels or tiers, with Tier 1responders serving as the frontlines to monitor security endpoints and perform incident triage procedures in line with the institution's incident response plans and procedures. Depending on incident classification, security events are then escalated to Tier 2 and Tier 3 responders accordingly to conduct deep-dive analysis and investigation to quickly remediate, contain and recover from the incident. The SOC's major functions commonly cover detect, respond, and recover phases in the information security cycle. These include network, host, and application activity monitoring; forensic investigation; threat analysis and modeling; and engagement with security service providers and information sharing groups. The BSFI should adopt adequate policies and procedures in managing the SOC which should be integrated into its governance mechanisms, business and IT operations, incident response and BCM processes.

Considering that it may be difficult for some organizations to establish a mature and fully-operational SOC with the requisite skills, expertise and tools, the BSFI may opt to outsource some or all of its SOC functions to a third party service provider. This may be under a managed security service arrangement either on-premise, off-premise or through cloud computing platforms. In this regard, Management should exercise adequate oversight, due diligence and other risk management controls, and comply with existing Bangko Sentral regulations on outsourcing and cloud computing.

4.1.2 **Emerging Technologies and Innovation.** Emerging technologies and innovation are continuously being introduced in the market resulting to a dynamic operating environment for BSFIs. These include distributed ledger technologies (DLT), cryptocurrencies, big data and internet of things (IOT), among others. These technologies, if prudently harnessed, can significantly increase market share, improve customer experience, enhance security, and promote financial inclusion.

Prior to adopting these emerging technologies, Management should fully understand the mechanics, implications to consumer protection, money-laundering and overall security posture as well as inherent risks associated with these new technologies. In

cases where applicable regulations/requirements are unclear, BSFIs should consult the Bangko Sentral prior to implementation.

4.2. **Information Sharing and Collaboration.** With the stealthier, sophisticated and advanced forms of cyber-threats and attacks confronting the financial services industry, BSFIs should have a collective, coordinated, and strategic response through information sharing and collaboration. Information sharing allows BSFIs to enhance threat intelligence/ situational awareness that enable quick identification, prevention, and response to emerging and persistent threats. In some cases, BSFIs may need to cooperate with concerned government/regulatory bodies, law enforcement agencies and third party providers to prosecute cyber-criminals, activate government incident response plans or issue warnings/advisories to the public. The extent, breadth, and nature of information sharing activities of BSFIs largely depend on their maturity and capabilities. Moderate to Complex BSFIs should actively engage in information sharing organizations and fora within the financial services industry.

At a minimum, BSFIs should define information sharing goals and objectives aligned with their ISSP and ISP. Further, BSFIs should formulate policies and procedures on information sharing activities within and outside their organizations, taking into consideration the following:

a. Obtaining Board and Senior Management approvals prior to joining information sharing groups/communities;
b. Listing/identifying threat information (i.e. indicators of compromise (IOC), tactics, techniques and procedures (TIPs), security alerts, etc.) that can be shared with trusted parties;
c. Establishing processes to sanitize/anonymize threat information that may contain sensitive/confidential data; and
d. Ensuring compliance with applicable laws, rules, and regulations (e.g. data privacy and bank secrecy laws).

4.3. **Continuous Improvement.** The BSFI should integrate continuous improvements in its ISSP and ISP to maintain an effective security posture amidst changing threat landscape and technological developments. Lessons learned from their own experiences as well as from other BSFIs/organizations should be incorporated in further enhancing its capabilities to identify, assess, and manage security threats and vulnerabilities. A holistic and systematic approach should be adopted in assessing the BSFI's security posture, supported by robust and effective metrics, to ensure that security program, initiatives and efforts are moving in the right direction. The improvement process should cover all aspects of ISRM, people, policies, standards and procedures, processes and technology which should ultimately result to ongoing cyber-resilience.

Footnotes

1. US National Institute of Standards and Technology (NIST), ISO, US FFIEC, COBIT and CPMI publications, among others.
2. Refers to the exploit of zero-day vulnerability which takes place on the same day the vulnerability becomes generally known. It also means zero days between the time the vulnerability is discovered and the first attack.
3. Application whitelisting is the maintenance and use of a list of applications and their components (e.g., libraries and configuration files) that are authorized to be present or active on a system according to a well-defined baseline.
4. Network and data flow diagrams should identify hardware, software, and network components, internal and external connections, and types of information passed between systems to facilitate the development of a defense-in-depth security architecture.
5. Degaussing is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.