BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 951
Series of 2017

Subject : Guidelines On Business Continuity Management

The Monetary Board, in its Resolution No. 369 dated 2 March 2017, approved the following guidelines on business continuity management for Bangko Sentral ng Pilipinas (BSP)-supervised financial institutions (BSFIs) and amendments in the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI).

Section 1. Section X182/4182Q/4182N/4194P/4197S/4176T on **Business Continuity Management** are hereby added to the MORB/MORNBFI to read as follows:

Section X182/4182Q/4182N/4194P/4197S/4176T Business Continuity Management; Policy Statement. BSFIs can be adversely affected by disruption of critical operations due to internal and external threats, which may be natural, man-made or technical in origin. Extreme events may cause major disruptions whose impact are very broad in scope, duration or both and can pose a substantial risk to the continued operation of BSFIs. Because BSFIs play a crucial role in the financial system and economy as a whole, it is important to ensure that their operations can withstand the effects of major disruptions. Thus, BSFIs need to have a comprehensive business continuity management (BCM) process as an integral part of their operational risk management system. A well-designed BCM process enables BSFIs to resume critical operations swiftly and minimize operational, financial, legal, reputational, and other material risks arising from a disruption. This also helps mitigate systemic risks as well as maintain public trust and confidence in the financial system.

Section 2. Subsection X182.1/4182Q.1/4182N.1/4194P.1/4197S.1/4176T.1 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.1/4182Q.1/4182N.1/4194P.1/4197S.1/4176T.1 ***Purpose, applicability, and scope.*** The guidelines aim to promote sound management of business continuity risks. These align existing regulations, to the extent possible, with leading standards and recognized principles on BCM, and shall serve as the Bangko Sentral's baseline requirement for all BSFIs.

The guidelines shall apply to BSFIs which include banks, non-banks with quasi-banking function (NBQB), non-bank electronic money issuers and other non-bank institutions which under existing Bangko Sentral rules and regulations and special laws are subject to Bangko Sentral supervision and/or regulation. Moreover, subject guidelines shall also apply to BSFIs with offshore data processing as may be appropriate to their situation.

Section 3. Subsection X182.2/4182Q.2/4182N.2/4194P.2/4197S.2/4176T.2 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.2/4182Q.2/4182N.2/4194P.2/4197S.2/ 4176T.2 ***Definition of terms.*** In these guidelines, terms are used with the following meanings:

a. *Alternate and Business Recovery Sites* shall refer to standby facilities for use during disruption of critical operations to ensure business continuity. These provide work space and/or the necessary technology environment needed to process business-critical information. Organizations may have more than one (1) alternate site. In some cases, alternate sites may involve facilities that are used for normal day-to-day operations but which are able to accommodate additional business processes when a primary location becomes inoperable. Examples of alternate sites include relocation and disaster recovery sites, whether managed directly or maintained by a third party for a BSFI or for use by multiple organizations.

b. *Business Continuity* shall refer to a state of continued, uninterrupted operation of a business.

c. *Business Continuity Management (BCM)* shall refer to an enterprise-wide framework encompassing policies, standards, facilities, personnel and practices that provides for continuous functioning of the institution during disruptions. It is proportionate to the BSFI's internal and external risk exposures and tailored to the nature, scale, and complexity of its business.

d. *Business Continuity Plan (BCP)/Plan* shall refer to a documented plan detailing the orderly and expeditious process of recovery, resumption, and restoration of business functions in the event of disruptions. It should be able to cover and establish linkages among its multiple components, such as communication plan, crisis management plan, contingency funding plan, and technology recovery plan.

e. *Business Impact Analysis (BIA)* shall refer to the process of identifying and measuring (quantitatively and qualitatively) the business impact or loss of business processes in the event of a disruption. It is used to identify recovery priorities, recovery resource requirements, essential staff, and dependencies (internal and external) to be incorporated in the plan.

f. *Crisis* shall refer to a situation that requires urgent action due to its disruptive impact on the BSFI's core activities or business and operating environment.

g. *Crisis Management Plan (CMP)* shall refer to a documented plan detailing the actions to be taken when a crisis strikes a BSFI and designed to maintain order amidst the confusion surrounding such situations. During and immediately after a crisis, the members of the crisis management team will convene and activate the plan to attain control over the crisis and minimize its impact to operations.

h. *Critical Process* shall refer to any activity, function or service, which when lost would materially affect the continued operation of the BSFI.

i. *Cyber Resilience* shall refer to an organization's ability to anticipate, handle, adapt to, and/or recover from evolving cyber threats.

j. *Events* shall refer to disruption scenarios such as loss of people, technology, alternate site, and service providers.

k. *Pandemic* shall refer to epidemics or outbreaks in humans of infectious diseases that have the ability to spread rapidly over large areas, possibly worldwide.
l. *Recovery Point Objective (RPO)* shall refer to acceptable amount of data loss should a disruption occur without severe impact on the recovery of operations.
m. *Recovery Time Objective (RTO)* shall refer to the period of time following an incident within which a product, system or business process must be resumed or resources must be recovered.
n. *Resilience* shall refer to the ability of an organization to anticipate, handle, adapt to and/or recover from a disruption and resume operations.
o. *Risk Assessment* shall refer to the process involving the identification and assessment of potential threats and vulnerabilities that could severely interrupt a BSFI's business activities and the corresponding likelihood and magnitude of impact on business processes.
p. *Technology Recovery Plan (TRP)/Disaster Recovery Plan (DRP)* shall refer to a documented plan detailing the technology strategy and requirements during recovery for business and support functions. The relevant regulations are in Subsection 3.3.2.13 of *Appendix 75d* of the Manual of Regulations for Banks (MORB) and *Q-59d* of the Manual of Regulations for Non-Bank Financial Institution (MORNBFI).

Section 4. Subsection X182.3/4182Q.3/4182N.3/4194P.3/4197S.3/4176T.3 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.3/4182Q.3/4182N.3/4194P.3/4197S.3/4176T.3 ***Roles and responsibilities.***

a. *Board of Directors and Senior Management.* The BSFI's board and senior management are responsible for overseeing the implementation of a sound BCM process, which involves the creation and promotion of an organizational culture that places high priority on business continuity. This should be reinforced by providing sufficient financial and human resources associated with the BSFI's business continuity initiatives. Senior management should establish BCM policies, standards, and processes, which must be duly endorsed to and approved by the board.

   Awareness training and periodic reporting to board and senior management on matters related to business continuity are equally important to ensure their continuing commitment and support. At a minimum, periodic management reports should include the following: (1) implementation status of the BCP; (2) incident reports; (3) plan test results; (4) changes to the plan; and (5) related action items to strengthen the BSFI's ability to recover during disruptions.

b. *BCM Coordinator/Unit.* Coordination and supervision of all business continuity activities should be assigned to a competent individual and/or unit with technical knowledge and experience consistent with the nature and complexity of the

BSFI's business activities. A complex[1] BSFI may need a BCM unit with a team of departmental liaisons throughout the organization. For a simple BSFI, an individual BCM coordinator may suffice. While the BCM coordinator/unit may recommend initiatives or activities to be prioritized, the board and senior management are ultimately responsible for understanding the critical business processes and subsequently establishing plans to meet business process requirements in a safe and sound manner.

c. *BSFI Personnel.* BSFI personnel should understand their roles and responsibilities on the prevention of crisis and recovery of business operations during disruptions. Business and support functions should allocate responsibilities for managing disruptions and provide clear guidance regarding the succession of authority to account for unavailability of key personnel in the event of a disruption.

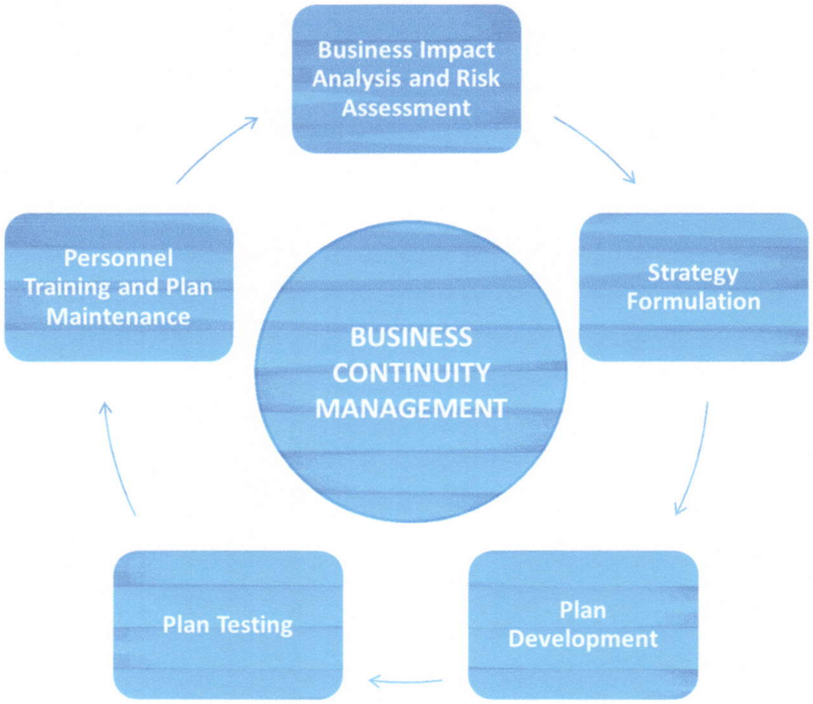
d. *Audit.* An independent review of the BSFIs' BCM framework and corresponding plans should be periodically performed with frequency based on a sound risk assessment process. This is to ensure that significant policy revisions resulting from changes in the operating environment, lessons learned from plan tests, and internal and regulatory audit recommendations have been considered. Moreover, plan testing exercises should be independently observed, verified, and evaluated to ensure reasonableness and validity of the testing process and the accuracy of test results.

Section 5. Subsection X182.4/4182Q.4/4182N.4/4194P.4/4197S.4/4176T.4 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.4/4182Q.4/4182N.4/4194P.4/4197S.4/ 4176T.4 ***Business Continuity Management Framework.*** BSFIs should adopt a cyclical, process-oriented BCM framework, which, at a minimum, should include five phases, namely: business impact analysis (BIA) and risk assessment, strategy formulation, plan development, plan testing, and personnel training and plan maintenance. This framework represents a continuous cycle that should evolve over time based on changes in business and operating environment, audit recommendations, and test results. This framework should cover each business function and the technology that supports it. Other related policies, standards, and processes should also be integrated in the overall BCM framework.

[1] Pursuant to Subsection X177.3 and 4177Q.3 MORB and MORNBFI, respectively. Non-bank financial institutions are classified as *"simple"* but maybe re-classified as *"complex"* depending on extent or degree of realiance of core business functions to technology.

Figure 1. Business Continuity Management Process


Business Impact Analysis and Risk Assessment
Strategy Formulation
Plan Development
Plan Testing
Personnel Training and Plan Maintenance
BUSINESS CONTINUITY MANAGEMENT

a. *Business Impact Analysis and Risk Assessment.* A comprehensive BIA and risk assessment should be undertaken to serve as the foundation in the development of the plan. The BIA entails determining and assessing the potential impact of disruptions to critical business functions, processes, and their interdependencies through work-flow analyses, enterprise-wide interviews, and/or inventory questions. Accordingly, the BSFI should determine the recovery priority, RTO, RPO, and the minimum level of resources required to ensure continuity of its operations consistent with the criticality of business function and technology that supports it. The BSFI should then conduct risk assessment incorporating the results of the BIA and evaluating the probability and severity of a wide-range of plausible threat scenarios in order to come up with recovery strategies that are commensurate with the nature, scale, and complexity of its business functions.

   Domestic Systemically Important Banks (DSIBs). To minimize the extent or impact of a DSIB's failure in the financial system, BSFIs identified as DSIB by the Bangko Sentral, pursuant to Subsec. X115.5 of the MORB and 4115Q.5 of the MORNBFI, should set the RTO for each of their critical processes to a maximum of four (4) hours from the point of disruption. For non-DSIB BSFIs, the RTO of critical processes should be primarily driven by their BIA and risk assessment.

b. *Strategy Formulation.* Recovery and resumption strategies to achieve the agreed time-frame and deliver the minimum required services as identified in the BIA should be defined, approved, and tested. The minimum requirements for the provision of essential business and technology service levels during disruptions should be established by concerned business and support functions.

   (1) *Recovery Strategy.* As business resumption relies primarily on the recovery of technology resources, adequate provisions should be in place to ensure

systems availability and recoverability during disruptions as prescribed under *Appendix 75d* of the MORB and *Q-59d* of the MORNBFI. Recovery strategies should be able to meet the agreed requirements between business units and support functions for the provision of essential business and technology service levels.

(2) *Continuity of Operations/Business Resumption Strategy.* The business continuity models adopted by the BSFI to handle prolonged disruptions should be based on the risk assessment of its business environment and the characteristics of its operations. The resumption strategies and resource requirements should be approved by the board as recommended by senior management or the relevant board committees to ensure alignment with corporate goals and business objectives.

c. *Plan Development.* Plans are an important, tangible evidence of the BSFI's business continuity initiatives. The objective of the plan is to provide detailed guidelines and procedures on response and management of a crisis, recovery of critical business services and functions and to ultimately resume to normal operations. The plan should be formulated on an enterprise-wide basis, reviewed and approved by the board and senior management at least annually and disseminated to all concerned employees. The plan should include provisions for both short-term and prolonged disruptions.

A well-written plan should describe the various types of events or scenarios that could prompt BCP activation. It should include, at a minimum, the following components:

(1) Escalation, declaration and notification procedures;

(2) Responsibilities and procedures to be followed by each continuity or recovery teams and their members. The procedures should enable the BSFI to respond swiftly to a crisis (i.e., a crisis management plan) and to recover and resume the critical processes outlined in the plan within the stipulated time frame during disruptions;

(3) A list of resources required to recover critical processes in the event of a major disruption. This would include, but not limited to: (a) key recovery personnel; (b) computer hardware and software; (c) communication systems; (d) office equipment; and (e) vital records and data;

(4) Relevant information about the alternate and recovery sites; and

(5) Procedures for restoring normal business operations. This should include the orderly entry of all business transactions and records during disruption into the relevant systems up to completion of all verification and reconciliation procedures.

Communication is a critical aspect of a BCP. In this respect, the BSFI should include a communication plan for notifying all relevant internal and external stakeholders (e.g., employees, customers, vendors, regulators, counterparties, and key service providers, media and the public) following a disruption. The BSFI should maintain an up-to-date call tree and contact list of key personnel and service providers, including communication flow and channels for internal and external stakeholders. Clear and effective communication will facilitate escalation for appropriate management action and instruction to all concerned and help manage reputation risks. The BSFI 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.

A crisis management plan should be included in the BCP to assist senior management in dealing with and containing an emergency and avoid spillover effects to the business. Senior management should identify potential crisis scenarios and develop corresponding crisis management procedures. This includes identifying a mix of individuals from various departments who are authorized to make instantaneous decisions during crisis situations. This team shall be responsible for the actual declaration of an event, activation of the plan, and internal and external communication process.

When outsourcing plan development, management should ensure that the chosen service provider has the expertise required to analyze the business needs of the BSFI and that the arrangement conforms with legal and regulatory requirements. The service provider should be able to design executable strategies relevant to the BSFI's risk environment and design education and training programs necessary to achieve successful BCP deployment.

d. *Plan Testing*

(1) *Types of Testing Methods.* Plan testing is a vital element of the BCM. It ensures that the plan remains accurate, relevant, and operable. Tests should be conducted periodically, with the nature, scope, and frequency determined by the criticality of the applications, business processes, and support functions. In some cases, plan tests may be warranted due to changes in BSFI's business, responsibilities, systems, software, hardware, personnel, facilities, or the external environment.

Testing methods can vary from simple to complex each bearing its own characteristics, objectives, and benefits. Types of testing methods in order of increasing complexity include:

(a) *Tabletop Exercise/Structured Walk-Through Test* – the primary objective is to ensure that critical personnel from all areas are familiar with the plan and that it accurately reflects the BSFI's ability to recover from a disruption.

(b) *Walk-Through Drill/Simulation Test* – similar to a tabletop exercise but with a more focused application. During this test, participants choose a specific scenario to which relevant plan provisions shall be applied.

(c) *Communication/Call Tree Test* – an exercise that validates the capability of crisis management teams to respond to specific events and the effectiveness of the call tree notification process in disseminating information to employees, vendors, and key clients.

(d) *Alternate Site Test/Exercise* - tests the capability of staff, systems, and facilities, located at alternate sites to effectively support production processing and workloads.

(e) *Component Test/Exercise* – A testing activity designed to validate the continuity of individual systems, processes, or functions, in isolation.

(f) *Functional Drill/Parallel Test* – test to determine capability of alternate site and BSFI employees to support strategy as defined in the plan, which involves actual mobilization of personnel, establishing communications, and recovery processing.

(g) *Enterprise-wide Full-Interruption/Full-Scale Test* – the most comprehensive type of test encompassing the entire organization and requires activation of all the components of the plan at the same time to simulate a real-life emergency and processing data and transactions using back-up media at the recovery site.

(2) *Test Policy / Plan.* Testing should be viewed as a continuously evolving cycle. The BSFI should incorporate the results of BIA and risk assessment and work towards a testing strategy that increases in scope and complexity to address a variety of threat scenarios. Test scenarios should vary from isolated system failures to wide-scale disruptions and promote testing its primary and alternate facilities, as well as with key counterparties and third-party service providers.

A testing policy should define roles and responsibilities for the implementation and evaluation of the testing program. Test plans with predetermined goals and test criteria should be developed for each testing activity. It should clearly define the objectives of testing, identify the functions, systems, or processes to be tested and the criteria for assessing what constitutes a successful test. Formal testing documentation (i.e., test plans, test scenarios, test procedures, test results) should be prepared to ensure thoroughness and effectiveness of testing and properly maintained for audit and review purposes.

(3) *Annual Enterprise-Wide Business Continuity Testing.* The BSFI must conduct an enterprise-wide business continuity test at least annually, or more frequently depending on changes in the operating environment, to ensure

its plan's relevance, effectiveness, and operational viability. The scope of testing should be comprehensive to cover the major components of the plan as well as coordination and interfaces among important parties.

(4) *Analysis and Report of Test Result.* Plan tests, including successes, failures, and lessons learned, should be thoroughly analyzed to promote continuous BCM improvement. Exceptions noted should be documented and corrective actions should be closely monitored to ensure that they are implemented in a timely manner by concerned parties, including the board and senior management, business line management, risk management, IT management, and other internal stakeholders.

e. *Personnel Training and Plan Maintenance.*

(1) *Training Program.* A business continuity training program should be provided to all concerned employees to promote awareness, familiarity, and understanding of their roles and responsibilities in the event of a disruption. The training program should be offered on a continuing basis for existing and new employees and should be updated to address changes to the plan.

(2) *Plan Maintenance.* Plans and results of BIA and risk assessment should be reviewed and updated on an ongoing basis (at least annually or when necessary) so that they remain consistent with the BSFI's current operations and business strategies. BCM-related documents (i.e., BCP, test program, policy guidelines, and program requirements) should be subject to change management process to ensure these are updated with proper approval and documentation with respect to any significant changes in the business environment or as a result of audit findings.

Section 6. Subsection X182.5/4182Q.5/4182N.5/4194P.5/4197S.5/4176T.5 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.5/4182Q.5/4182N.5/4194P.5/4197S.5/ 4176T.5 *Other policies, standards and processes.* The following policies, standards and processes should be integrated into the BCM process:

a. *Pandemic Planning.* Similar to natural disasters or technical disruptions, pandemics may also interrupt a BSFI's business activities. However, the difficulty in determining a pandemic's scope and duration present additional challenges in ensuring resilience and continuity of a BSFI's operations.

Generally, pandemic plans are integrated in the BSFI's BCP and follows the same BCM process with additional considerations, such as:

(1) *Business Impact Analysis and Risk Assessment.* The BCM process should consider pandemics as early as the BIA and risk assessment phase. The BIA and risk assessment should be updated to incorporate complexities that may arise from pandemics, such as (a) increasing level of absenteeism based on a

pandemic's severity; and (b) the need for another layer of contingency plans as regular disaster or emergency response methods are no longer feasible.

(2) *Strategy formulation.* To complement strategies for natural and technical disruptions, the following should be given due consideration when planning for pandemics:

(a) Trigger events – Trigger events and strategies should be defined depending on the nature of a pandemic. Pandemic planning should have the flexibility to accommodate varying degrees of epidemic or outbreak as pandemics normally occur in waves or phases and of varying severity.

(b) Remote access capability – In the event of a pandemic, enabling remote access may be one of the primary strategies available to a BSFI. To support a telecommuting strategy, the BSFI should ensure adequate capacity, bandwidth and authentication mechanisms in its technological infrastructure against expected network traffic or volume of transactions.

(c) External parties – With pandemics not limited to the BSFI, establishing working relationships with external parties is an essential component. In addition to the communication plan for all relevant internal and external stakeholders, the BSFI should establish open relationships and communication channels with local public health and emergency response teams or other government authorities. The BSFI should inform concerned parties of any potential outbreaks and, at the same time, be aware of any developments in the expected scope and duration of a pandemic.

(d) Employee awareness – As information becomes available from reputable sources or local agencies, the BSFI should ensure that steps to limit or reduce the risk of being affected by the pandemic are cascaded to its employees.

(3) *Plan Development.* Pandemic plans should be commensurate to the nature, size and complexity of a BSFI's business activities and have sufficient flexibility to address the various scenarios that may arise. At a minimum, the pandemic plan should include:

(a) Strategy that is scalable dependent on the extent and depth of the outbreak;

(b) Preventive measures, including monitoring of current environment and hygiene tools available to employees;

(c) Communication plan with internal and external stakeholders, including concerned local public health teams and government agencies; and

(d) Tools, systems and procedures available to ensure continuity of its critical operations even with the unavailability of BSFI's staff for prolonged periods.

(4) *Plan Testing.* Test policy/plan should include strategies to assess capability to continue critical operations, systems and applications even in the event of

a severe pandemic. When regular tests are unable to cover pandemic scenarios, separate pandemic plan tests should be carried out.

(5) *Personnel Training and Plan Maintenance.* The plan should be updated as developments and information become available. As needed, employee training programs should cover pandemic risks, including the roles and responsibilities of each employee during pandemic situations.

b. *Cyber Resilience.* Cyber-threats and attacks against the financial services industry have become increasingly widespread, sophisticated and coordinated. Recent cyber-attacks worldwide highlight, not only the degree of disruption to a BSFI's operations, but also the extent of reputational damage which could undermine public trust and confidence. As such, the BSFI should consider the potential impact of these cyber events into its BCM process and institute adequate cyber resilience capabilities.

Given the unique characteristics of cyber-threats and attacks, traditional back-up and recovery arrangements adopted by the BSFI may no longer be sufficient and even increase the damage to the BSFIs' network, operations and critical information assets. In worst case scenarios, back-up systems and alternate recovery sites are likewise affected rendering both sites inoperable. To ensure cyber resilience, 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. Defensive strategies and innovative recovery arrangements should be explored that are commensurate with the BSFI's cyber-security risk exposures and aligned with its information security program in accordance with *Appendix 75b* of the MORB and *Q-59b* of the MORNBFI.

c. *Information Security.* Mitigation strategies should consider security controls to manage risks that may arise once an event triggers plan activation. Security during disasters and disruptions is an important consideration to manage risks arising from the change in working environment. The relevant guidelines/standards on information security that may be considered in strategy formulation and/or in choosing alternate sites are in *Appendix 75b* and *Q-59b* of the MORB and MORNBFI, respectively.

d. *Interdependencies.* An effective plan coordinates across its many internal and external components, identifies potential process or system dependencies, and mitigates risks from interdependencies. The BSFI may have very complex operating and recovery environment wherein interdependencies need to be duly considered, such as telecommunications, third party service providers, and recovery site. Given the critical resources and services that are being shared with the BSFI or other entities, additional mitigating controls and recovery strategies need to be integrated in the plan.

e. *Liquidity Risk Management.* Sound liquidity risk management practices enable a BSFI to maintain availability of funds even in times of financial stress or adverse changes in market conditions. In the event of a business disruption, sound liquidity risk management practices should similarly apply. The BSFI should ensure it has sufficient liquidity to support its recovery strategies and continue supporting the delivery of basic banking services to the clients pending full business resumption. Guidelines on liquidity risk management are in *Appendix 74* and *Q-44* of the MORB and MORNBFI, respectively.

f. *Project Management.* Senior Management should ensure that availability and business continuity requirements are considered at the planning and development stages of new business products and services and other critical technology processes, such as systems development and acquisition, and change management.

g. *Event/Problem Management.* Operations personnel should be properly trained to recognize events that could trigger implementation of the plan. Although an event may not initially activate the plan, it may become necessary as conditions and circumstances change. Management should train and test BSFI personnel to implement and perform appropriate business continuity procedures within the timeframes of the plan.

h. *Outsourcing.* When a BSFI enters into an outsourcing arrangement, it should put due consideration on the business continuity and disaster recovery arrangements of the service provider to ensure continuity of operations. Detailed guidelines/standards on business continuity considerations for outsourcing arrangements are in *Appendix 75e* and *Q-59e* of the MORB and MORNBFI, respectively.

i. *Insurance.* Insurance is an option available to a BSFI for recovery of losses that cannot be completely prevented and the expenses related to recovering from a disruption. The BSFI should regularly review the adequacy and coverage of its insurance policies in reducing any foreseeable risks caused by disruptive events, such as loss of offices, critical facilities and equipment, and casualty. Insurance policies may also need to address the BSFI's legal responsibilities for failing to deliver services to its customers and counterparties. To facilitate the claims process, the BSFI should create and retain a comprehensive hardware and software inventory list in a secure off-site location and detailed expenses should be documented to support insurance claims.

Section 7. Subsection X182.6/4182Q.6/4182N.6/4194P.6/4197S.6/4176T.6 are hereby added to the MORB/MORNBFI to read as follows:

Subsection X182.6/4182Q.6/4182N.6/4194P.6/4197S.6/ 4176T.6 ***Supervisory Enforcement Actions.*** BSFIs should make available all policies and procedures and other documents/information related to the foregoing during on-site examination as well as provide copies thereof to the regulator when a written request is made to determine compliance.

Consistent with Section X009/4009Q/4009T, the Bangko Sentral may deploy enforcement actions to promote adherence with the requirements set forth in Section X182/4182Q/4182N/4194P/4197S/4176T of the MORB/MORNBFI and bring about timely corrective actions. The Bangko Sentral may issue directives to improve the BCM process, or impose sanctions to limit the level of or suspend any business activity that has adverse effects on the safety and soundness of the BSFI, among others. Monetary and non-monetary sanctions, as provided under existing laws, Bangko Sentral rules and regulations, may likewise be imposed on a BSFI and/or its directors, officers and/or employees for violation of subject Section X182/4182Q/4182N/4194P/4197S/ 4176T of the MORB/MORNBFI.

Section 8. ***Transitory Provision.*** The following provision shall be incorporated as a footnote to Section X182/4182Q/4182N/4194P/4197S/4176T:

BSFIs shall comply with the foregoing standards on BCM within a period of one (1) year from the effectivity of this issuance. In this regard, a BSFI should be able to show its plan of actions with specific timelines, as well as the status of initiatives being undertaken to fully comply with the provisions of Section X182/4182Q/4182N/4194P/4197S/ 4176T of the MORB/MORNBFI, upon request of the Bangko Sentral starting July 2017.

Section 9. ***Effectivity.*** This circular shall take effect fifteen (15) days following its publication either in the Official Gazette or in a newspaper of general circulation in the Philippines.

FOR THE MONETARY BOARD:

Ma. Cyd N. Tuaño-Amador

MARIA ALMASARA CYD N. TUAÑO-AMADOR
Officer-in-Charge

20 March 2017