Guide in Developing and Implementing an IT Risk Management Program

A. INTRODUCTION

Rural banks have become dependent more and more on technology in order to provide its customers banking products and services and at the same time enhance and streamline its banking operations. It is imperative that an IT Risk Management program be developed and implemented to support these technology-based/digital transformation initiatives to ensure that banks are prepared with controls in place to mitigate the business risks associated with any technology-based operations, and are quickly able to take action should new risks or threats arise out of these initiatives.

This document is based on the BSP's IT Risk Management Framework Circular 808 and is intended as a simplified guide for the rural banks to develop and implement their respective IT Risk Management program. This contains:

a. IT Risk Management Program Checklist;
b. General IT Risks and its Business Impact by Major Areas such as governance, operations, information/data security, electronic banking products and services, business continuity, vendor/outsourcing, system acquisition and implementation; and
c. Templates that shall serve as a guide and starting point in developing the required policies, guidelines and procedures defined in the IT Risk Management Framework.

The IT Risk Management Program Checklist lists down the activities needed to implement the program.

The General IT Risks by Major Areas simplifies the risk identification and assessment process needed to come up with the plan and the priorities. Bank needs to determine the probability of occurrence of the identified risks and level of impact the risks are to the bank.

The Templates provide a guide on what needs to be covered in each major area and already includes general policies and guidelines which the banks may adopt or modify as may be applicable to the bank practices and on how the bank intends to implement such policies. Procedures and additional guidelines, where necessary, still need to be developed by the banks to support the policies and guidelines provided.

The IT Risk Management program should be integrated into the bank's enterprise-wide Risk Management plan.

The five (5) components in an IT Risk Management program include:

1. Governance Structure,
2. Risk Identification, Assessment and Planning,
3. Establish Policies, Standards and Procedures to Manage Risks,
4. Implementation of Risk Control Policies, Standards and Procedures, and
5. Tracking, Monitoring and Reporting Risks.

Governance structure defines the organizational structure, including roles and responsibilities in developing, implementing, administering and monitoring the IT Risk Management program. As part of governance, a well-documented set of policies, standards and procedures should also be put in place to guide the bank in the execution and management of the program.

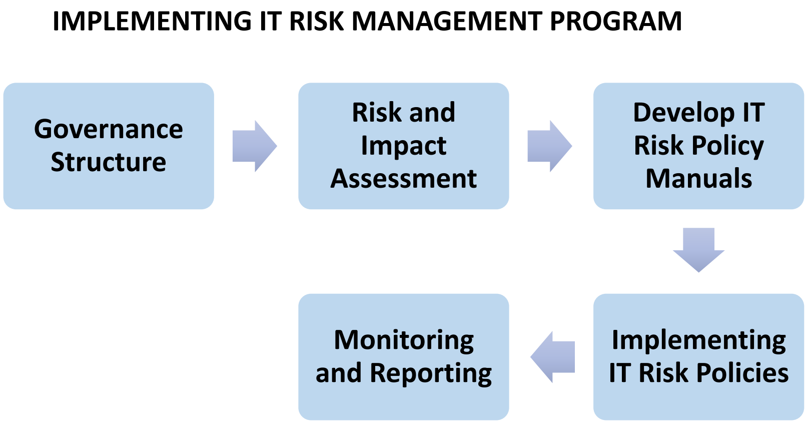
To establish a benchmark for the bank to identify the different risks, both current and potential, a risk identification and assessment should be conducted in order for a plan to be developed and be able to address and/or mitigate these risks, weaknesses and threats.

Once plan is in place and the risk control policies, standards and procedures have been documented and approved by the Board of Directors (BOD), these should be implemented to address and/or mitigate the risks identified giving priority in addressing risks with high impact and severity as well as those with high probability of occurrence.

As part of the program, implementation should be tracked, monitored and reported to the BOD on a regular basis to ensure any breaches or violations are immediately addressed and/or minimized, and possibly identify other existing and potential threats.

Refer to Annex 1 for the checklist in developing the IT Risk Management Program.

Figure 1: Process in Implementing IT Risk Management Program


IMPLEMENTING IT RISK MANAGEMENT PROGRAM
Governance Structure
Risk and Impact Assessment
Develop IT Risk Policy Manuals
Implementing IT Risk Policies
Monitoring and Reporting

B. SET UP ORGANIZATION STRUCTURE, ROLES AND RESPONSIBILITIES FOR GOVERNANCE

The Board of Directors (BOD) is ultimately responsible in knowing, identifying and understanding the risks, putting in place controls to address these risks and monitoring the actions taken to properly manage the risks. All plans and programs on IT Risk Management as well as related control policies, standards and procedures must be approved by the BOD.

Senior Management or Management Committee (ManCom) is responsible in developing, implementing, monitoring the execution of the enterprise-wide Risk Management plan, of which, the IT Risk Management program should be part of, and periodically report to the Board the status of the program.

Should ManCom decide to set up an IT Steering Committee (ITSC), ManCom can delegate this responsibility to the ITSC who will then be tasked to plan, develop, implement, monitor the execution of the program and reporting to the BOD. ITSC is also tasked to:

1. Develop the IT Strategic Plan,
2. Setup and organize the IT organization, including roles and responsibilities of the different IT functions, and
3. Develop, implement and monitor the IT control policies, standards and procedures.

In the absence of an ITSC, such responsibility can be assigned to one or two people, who are most capable from within in the bank. For example, the IT Strategic Plan can be delegated to the person in charge of business development or corporate planning. The Operations Head can be responsible in developing the required organization structure as well as the development and implementation of the policies, standards and procedures.

An IT Strategic Plan should always be based on or aligned with the bank's business plans and the bank's vision, say in the next two to three (2-3) years, from the development and approval of the IT Strategic Plan. The plan should be updated on an annual basis should there be changes made on the plans.

The bank's risk management unit or person responsible on risk management should closely work with each business unit to identify, measure, and monitor IT risks for each business unit on a periodic basis. Identified risks for the business unit should be acknowledged by the business unit head and mitigating controls and plans to reduce, if not totally eliminate, the risks are put in place, and execution of such plans and controls are monitored and reported to Senior Management and the BOD.

An independent body, IT Audit in particular, is tasked to review compliance to the IT Risk Management program, its policies, standards and procedures. IT Audit, which is part of the bank's Internal Audit unit, is to report directly to an Audit Committee, if available, or to the BOD directly. In the absence of an internal IT Audit, this can be outsourced to a third party who has the experience in conducting IT audits. This should be done, at the minimum, on an annual basis or when deemed necessary by Senior Management or the BOD when a breach or violation has occurred and where a special IT Audit needs to be conducted.

C. CONDUCT RISK IDENTIFICATION, ASSESSMENT AND PLANNING

The following types of business risks or impact to business are associated with any IT project and IT-enabled business operations:

1. Operational risk - risks due to failure of internal controls, personnel, IT systems and processes resulting in disruption in the delivery of the banks products and services,
2. Strategic risk - risks due to non-alignment of IT projects implemented and/or investments made with the strategic goals and directions of the bank resulting in cost and budget overruns and unmet business objectives,
3. Reputation risk - risks related to financial loss or damage to bank's reputation resulting in loss of trust and confidence in the bank, and
4. Compliance risk- risks resulting from non-conformity with regulatory requirements and banking-related laws resulting in corresponding penalties and sanctions to the bank.

All these risks have impact on the bank's earnings as well as capital. Risks can be existing or potential events that has an impact and consequence to the bank. Once risks are identified, an impact assessment is done for each risk to identify its consequences or impact to the bank. Probability of occurrence is then defined and together with the impact assessment, establishes the bank's exposure on the particular risk.

Annex 2 presents a list of general IT risks and should help start the risk identification process. The list is not comprehensive and the banks need to identify other risks that may apply to them specifically.

The tables below describe how to rate the impact, probability of occurrence and risk exposure. The results of the risk exposure sets the priorities in addressing the risks.

Table C-1: Risk Impact

Impact	Criteria
High	Consequences can be any of the following: 1. Stoppage of business operations or significant delay in opening up to start business day 2. System to support operations NOT available 3. Financial loss to the bank and/or client 4. Breach of system and data security with integrity and reliability of system and data compromised 5. Penalties and sanctions from regulatory bodies due to non-compliance to regulations

Impact	Criteria
Medium	Consequences can be any of the following: 1. Delay in system startup to support daily operations 2. Loss of system functionality due to error making part of the system partially available for use causing client inconvenience 3. Breach of system and data security but integrity and reliability of system and data NOT compromised 4. Warning from regulatory bodies due to non-compliance to regulations
Low	Consequences can be any of the following: 1. Minor system error with no loss of functionality 2. Loss of system functionality due to error making part of the system partially available for use causing bank personnel doing workaround or manual intervention

Table C-2: Probability of Occurrence

Probability	Criteria
High	It is almost certain or very likely that the risk will occur.
Medium	It is probable that the risk will occur (+/- 50 % chance of occuring).
Low	It is unlikely or improbable that the risk will occur.

Table C-3: Risk Exposure

Risk Exposure	Probability			
Impact		High	Medium	Low
	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

D. ESTABLISH POLICIES, STANDARDS AND PROCEDURES TO MANAGE IT RISKS

Using the results of the risk assessment made, policies, guidelines and procedures can be developed to address the identified risks and prioritized accordingly.

The establishment of the policies, guidelines and procedures will serve as the basis for IT governance and the bank's adherence to these is expected to minimize, if not totally eliminate risks related to IT projects, implementation and/or operations. This is to be enhanced on an ongoing basis as new risks or threats are identified or new areas need to be covered by new policies.

At the minimum, IT risk policies need to address the following:

1. What are the objectives of the policy document;
2. Who and what are covered by such policy document;
3. What are the policies and guidelines that need to be adhered to by those covered by the policy document; and
4. What are the procedures required to implement these policies and guidelines.

D1. **System Acquisition and Implementation** policies establish guidelines for bank personnel involved in system acquisition and implementation in the evaluation and selection of software to be acquired, including defining the selection criteria for acquisition, requirements in vendor contracts, and system implementation process (project management) to ensure that systems are implemented on time, within budget and meets the business objectives or purpose for which system is to be acquired or modified.

Refer to Annex III: System Acquisition and Implementation Template

D2. **IT Operations** policies establish guidelines for bank personnel involved in IT operations in order for IT systems and processes to run smoothly, safely and in an efficient manner that provides for accuracy, high system availability and reliability of the IT systems used. These policies should cover and address change management, incident and problem management, backup and recovery management, operations management on daily operations, periodic maintenance and capacity review, and help desk management.

Change Management policies set guidelines in handling software updates, patches and fixes that need to be deployed and implemented to eliminate any security risks if these are not implemented.

Incident and Problem Management policies set guidelines in handling incidents and problems encountered as to recording, reporting, monitoring and addressing reported incidents and problems until resolved or closed.

Backup and Recovery Management policies set guidelines in handling backup and recovery requirements to ensure integrity, reliability and availability of systems and data needed in order to meet system recovery time objectives as well as regulatory requirements for backup. At the minimum, these should define:

1. What to backup - systems only, data only, and both systems and data,
2. Frequency of backup - daily, weekly, monthly, and annual,
3. Backup location - onsite and offsite,
4. Type of storage/media - cloud, backup server and removable storage, and
5. Security of and access to backup.

Refer to Annex IV: IT Operations Template

D3. **Information Security** policies establish guidelines for **ALL** bank directors, officers and staff in the use and access of the bank's systems and data in order to maintain the confidentiality, integrity, reliability and availability of systems and data. These policies should cover and address physical and environmental protection, personnel security, security administration and monitoring, authentication and access control, systems and network security, use of encryption standards, malware prevention, remote access, security threats prevention and incident/problem management and control.

Physical and Environmental Protection policies set guidelines in the setting up and maintaining environmental facilities, physical security of and access to facilities where systems and data are located.

Personnel Security policies set guidelines in personnel recruitment, evaluation, selection and hiring, employee use and access of bank facilities,

Authentication and Access Control policies define the user's access rights and privileges to the bank's systems, includes hardware/servers, network and security equipment, and data based on "need to know and use" basis given their defined roles and responsibilities in the bank, method of user access, password definition and user authentication both for on premise and remote access, and control on default super user of all equipment and systems software.

Systems and Network Security policies define the setup, configuration requirements, administration and maintenance of all hardware/servers, network and security equipment, network topology.

Refer to Annex V: Information Security Template

D4. **Electronic Banking, Electronic Payment, Electronic Money and Other Electronic Banking Products and Services** policies establish guidelines in adopting an aggressive security posture, controls in administering and managing electronic services accounts to ensure confidentiality and integrity of information and records in the system, non-repudiation of transactions, security of the digital or electronic banking environment, and mitigate the impact of cyber fraud.

Refer to Annex VI: Electronic Banking Products and Services Template

D5. **IT Outsourcing and Vendor Management** policies establish guidelines for bank management to have an effective outsourcing oversight program in order to understand, monitor, measure, and control the risks associated with outsourcing. These should cover risk assessment, evaluation and selection of vendors, including criteria for vendor selection, contract review, monitoring of vendors based on service level agreement, and compliance to regulatory requirements.

Refer to Annex VII: IT Outsourcing and Vendor Management Template

D6. **Business Continuity Management (BCM) Program** establishes guidelines for **ALL** bank directors, officers and staff in disaster preparedness to ensure continuity, timely recovery and resumption of operations in case of business interruptions. An effective BCM defines the business impact on different disaster scenarios, recovery objectives and strategies, business continuity/disaster recovery plans, testing, training and maintenance of plans.

Refer to Annex VIII: Business Continuity Management Program Template

E. IMPLEMENT POLICIES, STANDARDS AND PROCEDURES TO CONTROL RISKS

Once approved by the BOD, the policies, standards and procedures should be disseminated and discussed with relevant officers and staff that should follow these procedures. For example, the Information Security policies and procedures should be discussed with all officers and staff as these are important and relevant for them to understand and follow.

F. TRACK, MONITOR AND REPORT RISK-RELATED OCCURRENCES AND EVENTS

Monitoring of IT activities and performance is important in determining if the controls put in place are effective or not. IT activities and performance are measured against the IT plans as well as against standards or benchmarks defined and approved by the BOD. Some of the activities that should be measured are:

1. For planned projects to be implemented, accuracy or correctness of implementation as agreed prior to start of the project, timeliness of delivery or implementation of project and actual costs as against budget are key measures that need be monitored,
2. Other performance measurements include system availability, network or online availability, response time to problem resolutions, among others are compared against standards or benchmarks defined, and
3. Compliance to approved internal policies and regulatory requirements.

Identified risks, security breaches and violations should be tracked until adequate measures or actions have been taken to address these risks or breaches.

A monthly report should be submitted and presented to the BOD while an IT Audit should be made at least on an annual basis. Special IT Audit may be conducted if serious breaches or violations happen which are considered reputational and/or compliance risks.

Annex I: IT RISK MANAGEMENT PROGRAM CHECKLIST

Program Activities	Responsible Unit	Status
Setup Organization Structure, Roles and Responsibilities		
Organization Structure		
Roles and Responsibilities Board of Directors Senior Management IT Steering Committee (if available) IT Head Risk Management Head Internal Audit Head		
Strategic Plan		
Conduct IT Risk Identification, Assessment and Planning		
Types of Risk		
Risk Identification and Assessment		
Action Plan to Mitigate Risks		
Establish Policies, Standards and Procedures		
System Acquisition and Implementation		
IT Operations		
Information Security		
Outsourcing and Vendor Management		
Electronic Banking Products and Services		
Business Continuity Plan		
Implement Policies, Standards and Procedures		
Education and Training		
Implementation		
Track, Monitor and Report		
Tracking and Monitoring Performance vs. Plans and vs. Service Levels		
Tracking and Monitoring Performance vs. Service Levels		
Management and Board Reporting		

Annex II: GENERAL IT RISKS BY MAJOR AREAS

Risks	Type of Risk	Likely Consequence to Business
Governance		
Absence of governance structure, standards and procedures to manage risks	Operational Strategic Compliance	• Lack of or no accountability and responsibility in managing risks • Failure to identify and address risks
Absence of IT Strategic Plan	Strategic Operational Compliance	Lack of or no clear direction in IT initiatives
Operations		
Natural calamities that cause flooding, power failure and the like	Operational	• No bank or branch operations • System availability and reliability are compromised or not available
Systems error	Operational	• System down or not available or system operational but with limited functions working depending on error severity • System integrity, availability and reliability are compromised
Unauthorized access to systems, servers, data center facilities	Operational Reputational	System integrity is compromised
Human error in processing	Operational	• System recovery needed or system operational with limited functions depending on error type • System integrity, availability and reliability are compromised
Malware, virus or denial of service attacks on the system	Operational	System integrity is compromised.
Insufficiency or incomplete backup	Operational	• Delay in system recovery when required • System integrity, availability and reliability are compromised
Absence of Operations policies and procedures on scheduling, executing, startup/shutdown, backup and restore, problem resolution and error handling	Operational	• Inconsistent processes adopted or used by operations • System integrity, availability and reliability are compromised • Difficult to audit
Connectivity to Core System down or not available	Operational	• Manual transaction processing in all branches • System integrity, availability and reliability are compromised

Lack of preventive maintenance and/or capacity monitoring	Operational	System availability and reliability are compromised
Absence of service levels required to support business requirements	Operational	System availability and reliability are compromised
Absence of audit trails in the handling and processing of data - from receipt of, processing of, access to, transmission of and storing of data		• System integrity is compromised • Difficult to audit
Information/ Data Security		
Unauthorized access to or sharing of data - data theft	Operational Reputational Compliance	Data privacy and confidentiality are compromised
System error	Operational Reputational	Data integrity is compromised
Insufficiency of or incomplete backup	Operational	Data integrity is compromised
Fraud	Operational Reputational Compliance	Data privacy and confidentiality are compromised
Human error in processing or handling of data	Operational Reputational Compliance	Data integrity is compromised
Absence of Information Security policies and procedures on authorization and access control, personnel security, infrastructure, facilities and environmental security	Operational Compliance	• Lack of or no accountability in ensuring data confidentiality, security and integrity • Data integrity is compromised • Difficult to audit
System Acquisition and Implementation		
Failure or delays in system implementation	Operational Strategic	Budget and cost overruns
Business objectives not met	Operational Strategic	Budget and cost overruns
Weakness in system testing or in system implementation process	Operational Strategic	System integrity and reliability are compromised
Weakness in automated system controls	Operational Strategic	System integrity and reliability are compromised
Absence of System Acquisition and Implementation policies and procedures on project management and system change management	Operational Compliance	• Lack of or no accountability and responsibility in implementing systems • System integrity and reliability are compromised • Difficult to audit

Outsourcing and Vendor Management		
Absence of Outsourcing and Vendor Management policies and procedures on vendor selection, contracts and service levels	Operational Compliance	• Poor or inadequate vendor management and performance monitoring • Inadequate provisions on controls in contract • Difficult to audit
Vendor failure to meet deadlines	Operational Strategic	Cost and budget overruns
Absence of vendor contracts, or contracts not reviewed by legal, responsibilities not clearly defined, service levels not defined	Operational Compliance	Vendors cannot be held accountable for their shortcomings
Vendor failure to comply with information security requirements (e.g. unauthorized access, compromised passwords) and service level agreements	Operational Compliance	• Confidentiality, security, integrity, availability and reliability of services compromised
Electronic Banking Services		
Absence of policies and procedures in implementing electronic banking services including lack of controls in customer verification, authentication and access privileges and non-repudiation of transactions	Operational Reputational Compliance	• Confidentiality, security, integrity, availability and reliability of services compromised • Financial loss to bank and client • Loss of trust in bank • Consumer protection and data privacy are compromised
Business Continuity		
Absence of disaster recovery site and/or contingency plans	Operational Strategic Compliance Reputational	• No bank or branch operations for long periods of time • Loss of trust in bank

Annex III: SYSTEM ACQUISITION AND IMPLEMENTATION

I. OBJECTIVES

a. To serve as guide in the evaluation and selection of vendor solutions and in managing the system/project implementation process

b. To ensure that due diligence is performed in the evaluation and selection process in any system acquisition, and controls are in place and implemented to meet business requirements, deadlines and budget during system/project implementation process

II. COVERAGE

These policies apply to bank personnel who will participate in system acquisition and implementation projects.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

a. Board of Directors - approves system acquisition and implementation policies and procedures and subsequent updates thereafter; approves any major system acquisition

b. Senior Management - provides oversight function to any system acquisition and implementation; provides periodic status updates on system implementation to the Board

c. Head of Information Technology - manages the technology part in system acquisition and implementation process until completion

d. Compliance Officer/Risk Management Officer - conducts reviews during the implementation process for compliance to internal policies and regulatory requirements and identifies risks, threats and vulnerabilities that may cause disruption or delays in implementation

e. Internal Audit - conducts post implementation audit review; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

1. Senior Management shall designate a Senior official to oversee major system acquisition and implementation projects and shall act as the overall Project Sponsor.

2. Any major system acquisition shall have prior Board approval.

System Evaluation and Selection

3. Business Requirements Definition shall be developed prior to any system evaluation and selection process.

4. Evaluation and selection process shall consider at least 3 vendor solutions to choose from.

5. Evaluation and selection criteria shall be defined, documented and include, among others, system capability to meet the minimum business requirements (must have) and/or at least 70-80 % of the all business requirements (must have and nice to have requirements) as well as vendor's experience in implementing the proposed solution, vendor's financial capability and vendor personnel technical capability to implement, maintain and support the proposed solution.

System Implementation

6. A Project/System Implementation Plan shall be developed prior to start of any system implementation activity. The plan shall include a timeline for all activities and responsible units and/or individuals, problem reporting and handling including escalation procedures, change request handling, among others.

7. System implementation shall adopt standard project management practices from project planning and Initiation, business requirements mapping, customization and/or development, systems and user acceptance testing, training and documentation, migration, implementation and post implementation review.

8. A regular project status meeting shall be conducted from project kickoff until project closure and periodic status reports prepared and submitted to Senior Management and the Board.

9. User Acceptance test conditions with their expected test results shall be defined prior to user testing and used as basis for system acceptance.

System Maintenance and Change Management

10. System changes shall be initiated by a documented change request and approved my Senior Management prior to execution.

11. System changes shall go through similar project management procedures prior to implementing such change into production.

12. A Software Maintenance Agreement shall be entered into with the software provider or be part of an annual subscription agreement that will provide software updates, patches and fixes to software problems.

Annex IV: IT OPERATIONS

I. OBJECTIVES

a. To serve as guide in managing IT Operations of the bank

b. To ensure that controls are in place and implemented in IT Operations that provides for reliable, available, secure and smooth day-to-day operations, and meets performance standards of the bank

II. COVERAGE

These policies apply to all IT personnel involved in the management and conduct of day-to-day IT operations.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

a. Board of Directors - approves IT operations policies and procedures and subsequent updates thereafter

b. Senior Management - provides oversight function on IT operations; provides periodic reports on performance to the Board

c. Head of Information Technology - manages IT operations and implements IT operations policies and procedures

d. Compliance Officer/Risk Management Officer -reviews compliance to internal IT operations policies and regulatory requirements and identifies new risks, threats and vulnerabilities

e. Information Security Officer/Data Privacy Officer - works with IT operations in implementing information security policies and procedures

f. Internal Audit - conducts annual audit review; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

Preventive Maintenance

1. A Hardware Maintenance Agreement shall be entered into with the provider of all computer, network and communications equipment after expiry of the warranty, that provides for a periodic preventive maintenance schedule on such equipment.

Change Management and Control

2. Changes in configuration and settings to computer equipment, network and communications equipment shall be recorded and tested in a controlled environment prior to implementing in production. Such changes shall be logged, tested before putting in production and monitored post production.

3. Replacement of computer equipment, network and communications equipment shall be tested in a controlled environment prior to replacing old equipment in production. Setting up the new equipment shall include hardening and/or configuring the equipment based on established configuration and hardening standards.

Patch Management and Control

4. Software updates, patches and fixes shall be recorded and tested in a controlled environment prior to implementing in production. Priority shall be given to updates, patches and fixes that has an impact on security. Critical or major updates, patches and fixes shall have prior authorization before implementing such changes.

Incident/Problem Management

5. Incidents or problems encountered shall be reported, recorded and/or logged, addressed within an acceptable timeframe depending on severity level, monitored until closure, and reported to Senior Management and where necessary, to the Board.

Scheduling

6. Schedule of program execution and operations activities shall be documented and maintained. Such schedules shall be developed for daily, weekly, monthly, quarterly and annual activities.

Systems and Data Backup

7. Systems in production shall be backed up at least quarterly and when changes have been made on the system. Included in this backup are the operating system, systems software, applications software, database and other programs needed for systems to perform its expected function.

8. Data shall be backed up daily. Data backup shall be kept for a defined period based on regulatory requirements for backup.

9. Systems and data backup shall be stored on both onsite and offsite locations.

10. Systems and data backup shall be tested at least semi-annually as to its reliability, availability and recoverability.

11. Inventory of backup media used shall be documented and updated at all times. Backup media shall be stored in a secured and controlled environment. Only authorized personnel

shall be allowed access to the backup media and environment where stored. Every such access shall be logged and monitored.

12. Backup and restoration procedures shall be documented, maintained and made available at both onsite and offsite locations.

Help Desk Support

13. Help Desk Support unit shall be setup to resolve, repair, fix software and hardware problems reported by bank personnel.

Annex V: INFORMATION SECURITY

I. OBJECTIVES

a. To serve as guide in the management of information security implementation in the bank

b. To ensure that information security controls are in place and implemented in regard to availability, confidentiality and integrity of information resources and systems used in the bank

II. COVERAGE

These policies apply to all bank personnel who will access and use the information resources and systems necessary to perform their duties and responsibilities.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

a. Board of Directors - approves information security policies and procedures and subsequent updates thereafter

b. Senior Management - provides oversight function on information security policy implementation; provides periodic updates to the Board especially reports on security breaches and violations

c. Heads of Business Units and Operations Units - implements information security policies and procedures

d. Compliance Officer/Risk Management Officer -reviews compliance to internal information security policies and regulatory requirements and identifies new risks, threats and vulnerabilities

e. Information Security Officer/Data Privacy Officer - develops and updates policies and procedures based on audit findings and new risks, threats and vulnerabilities identified; monitors information security policy implementation and reports security breaches and violations to Senior Management

f. Internal Audit - conducts annual audit review; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

Asset Classification and Control

1. An updated inventory shall be maintained of all hardware and software, with its owners clearly identified.

2. Information shall be classified as to restricted, confidential, internal or public and access to such information is based on classification.

Physical and Environmental Protection

3. All servers and network and communications equipment shall be stored in a secured and controlled environment, that is, in a lockable cabinet rack and located in a secure location. Only authorized personnel shall have physical access to servers, network and communications equipment. Access to the equipment inside the rack shall be logged, monitored and reported to the Head of Information Technology.

4. Environmental requirements on the use of servers, network and communications equipment shall be complied with at all times including provision for backup power using UPS and generator, fire suppression equipment and temperature and humidity control tools.

5. CCTV cameras shall be installed in strategic locations in all branches and monitored centrally.

Authentication and Access Control

6. Access rights shall be provided to its personnel based on job function, roles and responsibilities in the organization and on a 'need to know and use' basis. Prior approval shall be obtained before access rights are granted.

7. Personnel who will access computer resources (hardware, network and communications equipment, application software) shall be provided with unique username or user ID and password and shall be accountable and responsible for its use, protection and safekeeping. Default passwords shall be changed immediately on initial use of the username or user ID.

8. Default super usernames/user IDs and passwords shall be changed and assigned only to a Senior official and to be used only on initial setup of access rights or when required during recovery.

9. Bank personnel shall be responsible for the safekeeping and protection of his/her password, thus must keep them confidential. They should not divulge or share their passwords to others.

10. Passwords created shall have a minimum of 10 characters composed of a mix of upper case alphabets (A-Z), lower case alphabets (a-z), numbers (0-9) and special characters.

11. A Security Administrator shall be designated to define and maintain access rights, assign and maintain usernames or user IDs, monitor access to the computer resources especially unusual or unauthorized access, activities or attempts, and report such events to Senior Management.

12. Security Administrator shall have no other access rights except for the purpose indicated above.

Systems and Computer Equipment Security

13. Configuration and hardening standards shall be defined and implemented for computer equipment - servers, workstations (desktops and laptops) and mobile devices.

14. Hardening of servers shall be done prior to implementation of new systems.

Network and Communications Security

15. Configuration standards shall be defined and implemented for network and communications equipment, Local Area Network (LAN), Wide Area Network (WAN) and Wireless communications. This includes defining which packets, ports, protocols among others, allowed.

16. Changes in configuration shall be authorized prior to making such changes. Changes shall be logged, tested before putting in production and monitored post production.

Remote Access

17. Remote access to information resources and equipment shall require prior approval and to be provided only on as need basis and on specific resources and equipment and for a specified period of time.

18. Only authorized computer equipment and/or mobile devices shall be allowed remote access to information resources and equipment.

19. Remote access activities shall be logged and monitored at all times by the immediate supervisor.

Encryption

20. The use of industry-accepted encryption algorithms shall be implemented where data needs to be secured and protected from data capture, transmission, storage, retrieval and disposal.

21. The generation, storage, entry, use and assignment of keys used for encryption shall be protected and secured.

Malicious Code Protection

22. All computer equipment shall use industry standard anti-virus or malware prevention software and must be updated at all times on the computer equipment where installed.

Personnel Security

23. All employees shall be well informed and understand the information security policies.

24. Only applicants that meet the minimum qualification requirements shall be considered for the position.

25. Company shall conduct background and verification check on the applicant prior to hiring.

26. Personnel to be hired shall sign a Confidentiality and Non-Disclosure Agreement.

27. Personnel to be hired shall sign an Acceptable Use Policy Agreement that stipulates the proper use and safekeeping of company resources and observance of/adherence to information security policies and the adopt the practice of safe computing.

28. Newly hired personnel shall be educated on the information security policies and other relevant policies that may apply to the role and function of the position.

29. Personnel resigning or terminated shall obtain clearance from the different units prior to being given release papers.

Incident/Problem Management

30. Incidents or problems encountered shall be reported, recorded and/or logged, addressed within an acceptable timeframe depending on severity level, monitored until closure, and reported to Senior Management and the Board.

31. Bank personnel are expected and shall immediately report security breaches and/or violations and possible fraud to immediate supervisor and subsequently to Senior Management and where impact is to the bank, the Board shall likewise be immediately notified.

Annex VI: ELECTRONIC BANKING PRODUCTS AND SERVICES

I. OBJECTIVES

a. To serve as guide in managing the implementation of electronic banking products and services in the bank

b. To ensure controls are in place and implemented in regard to authorization and authentication, non-repudiation, confidentiality and integrity of electronic banking products, services and transactions

II. COVERAGE

These policies apply to bank personnel that are involved in the management and operations of electronic banking products and services.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

a. Board of Directors - approves electronic banking products and services implementation policies and procedures and subsequent updates thereafter; approves all electronic banking projects and ensures alignment with the bank's business objectives

b. Senior Management - provides oversight function to any electronic banking project; provides periodic performance updates on all electronic banking projects to the Board

c. Head of Information Technology - manages the technology part of electronic banking products and services offered by the bank to its customers

d. Compliance Officer/Risk Management Officer - conducts reviews during the implementation of electronic banking projects for compliance to the outsourcing agreement, internal policies and regulatory requirements and identifies risks, threats and vulnerabilities that may cause disruption in the outsourcing services provided

e. Internal Audit - conducts regular audit review; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

1. Senior Management shall designate a Senior official to manage the implementation of electronic banking products and services and monitor and report performance to Senior Management and to the Board.

2. An Operations Support Unit shall be created for purposes of addressing customer complaints, monitoring system performance, transaction reconciliation, card issuance, cash availability in ATMs, among others.

3. Clients shall agree to the terms and conditions in using electronic banking products and services.

Non-Repudiation

4. The bank shall use a digital certificate to ensure that transactions passing through the internet cannot be repudiated and presents undeniable proof of participation by both the client and the bank. The bank shall apply for a digital certificate from a trusted Certificate Authority.

Authorization Controls and Access Privileges

5. Access to electronic banking products and services shall require enrolment from the bank's clients. All client enrolment for the use electronic banking products and services shall be verified and approved by authorized bank personnel.

6. Clients shall assign a valid username and password to be used for logging in to the mobile or internet banking facility. Clients are responsible for the use, protection and safekeeping of their username and password.

7. Passwords created shall have a minimum of 10 characters composed of a mix of upper case alphabets (A-Z), lower case alphabets (a-z), numbers (0-9) and special characters.

8. Clients shall be provided with an ATM debit card to be used for transactions done through an Automated Teller Machine (ATM) or Point-of-Sale (POS) terminals. ATM debit cards issued shall be compliant with the Europay-Mastercard-Visa (EMV) standards using chip-based cards. A Personal Identification Number (PIN) is assigned to the card by the client and shall contain six (6) digits. Clients are responsible for the use, protection and safekeeping of their ATM card and PIN.

Confidentiality and Integrity of Information, Transactions and Records

9. Electronic banking products and services passing through the internet shall require the use of two-factor authentication for its transactions.

10. Transactions passing through the internet shall be encrypted end-to-end using Hyper Text Transfer Protocol Secure (HTTPS) and Transport Layer Service (TLS) as its encryption protocol.

11. Transactions passing through the ATM network shall be encrypted from ATM or POS terminal to the ATM card issuer bank for authorization and back to the ATM or POS terminal for consummation of the transaction. Transactions passing from one node to another node (from ATM acquirer bank to Bancnet ATM Switch Network, from Bancnet ATM Switch Network to ATM card issuer bank) within the Bancnet ATM Switch Network shall be encrypted using Public Key Infrastructure (PKI) of the participating acquiring and issuing banks as well as Bancnet.

12. Card and account numbers shall be masked and only the last 4 digits are shown at all times in receipts and in confirmation notices.

13. The bank shall provide for dual control in the use and safekeeping of encryption keys.

Application Security

14. The application shall provide notice or advise to the client for any data change, transactions completed or activities affecting the client's account. This can be done using email or SMS text message. System shall keep an audit trail of all such activities.

Infrastructure and Security Monitoring

15. CCTV devices shall be installed in ATM locations, where applicable.

Controls Over Fund Transfers/Payments

16. Third party accounts that will be used in transfers and payments shall require enrolment to eliminate encoding errors of 3rd party account information.

17. Third party account transfers and payments shall provide for a client option to set transfer or payment limits but shall not exceed limits set by the bank.

Controls on Specific Electronic Services and Channels

18. Automated Teller Machines (ATM) and Point of Sale (POS) Terminals shall comply with Philippine domestic EMV standards specifications.

Annex VII: OUTSOURCING AND VENDOR MANAGEMENT

I. OBJECTIVES

a. To serve as guide in the management of risks that are associated with outsourcing the bank's functions and services, in particular, in conducting vendor evaluation and selection process and in the execution all outsourcing engagements of the bank

b. To ensure that controls are in place and implemented during the execution of outsourcing/ vendor agreements of the bank

II. COVERAGE

These policies apply to bank personnel who will participate in the outsourcing engagement.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

f. Board of Directors - approves outsourcing and vendor management implementation policies and procedures and subsequent updates thereafter; approves all outsourcing and vendor engagements to be entered into

g. Senior Management - provides oversight function to any outsourcing engagement; provides periodic performance updates on outsourced services to the Board

h. Head of Information Technology - manages the outsourcing engagement; reports vendor performance vs. agreed service levels to Senior Management

i. Compliance Officer/Risk Management Officer - conducts reviews during the implementation of outsourcing engagement for compliance to the outsourcing agreement, internal policies and regulatory requirements and identifies risks, threats and vulnerabilities that may cause disruption in the outsourcing services provided

j. Internal Audit - conducts regular audit review; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

1. Senior Management shall designate one of its Senior officials to oversee and manage the outsourcing engagement.

2. Any outsourcing and vendor engagement shall have prior Board approval.

Vendor Evaluation and Selection

3. Outsourcing Requirements shall be developed prior to any outsourcing evaluation and selection process.

4. Evaluation and selection process shall consider at least 3 vendors to choose from.

5. Evaluation and selection criteria shall be defined, documented and include, among others, ability to meet the outsourcing requirements as well as vendor's experience in implementing the proposed solution, vendor's financial capability and vendor personnel technical capability to implement, maintain and support the proposed solution.

Outsourcing and Service Contracts

6. Outsourcing and service contracts shall have the following provisions:

   i. Scope of services,
   ii. Roles and responsibilities of both parties,
   iii. Service Level Agreement (SLA) including penalties for non-compliance to SLA,
   iv. Security standards,
   v. Adherence to law, regulatory requirements and internal policies and standards,
   vi. Incident handling and reporting for security breaches, violations and fraud including associated fines,
   vii. Business continuity provisions,
   viii. Provision to allow audit by regulators on the operations as well as financial information,
   ix. Termination clause,
   x. Confidentiality and data privacy clause,
   xi. Vendor Change of ownership,
   xii. Assurance that bank system and data is segregated from other clients and provider system and data,
   xiii. Commitment to infrastructure upgrades, and
   xiv. Insurance provided to protect client resources.

7. All outsourcing and service contracts shall be reviewed by legal.

8. Vendor performance based on agreed service levels as well as compliance to regulations shall be monitored and reported regularly to Senior Management.

Annex VIII: BUSINESS CONTINUITY PLAN (BCP)

I. OBJECTIVES

a. To serve as guide in the management of the bank's business continuity program

b. To ensure the bank's resilience to emergency or disaster situations and its capability to respond and continue business operations when emergency or disaster situations are encountered

II. COVERAGE

These policies apply to all bank personnel.

III. GOVERNANCE/ROLES AND RESPONSIBILITIES

a. Board of Directors - approves the Business Continuity Plan (BCP) and subsequent updates thereafter

b. Senior Management - provides oversight function in the development, testing, implementation and maintenance of the BCP; provides updates to the Board on the results of the BCP testing conducted

c. Compliance Officer/Risk Management Officer -reviews compliance to internal BCP policies and regulatory requirements and identifies new risks, threats and vulnerabilities

d. Internal Audit - conducts audit review during the BCP testing; provides report to the Audit Committee and the Board

IV. POLICIES AND GUIDELINES

1. A Crisis Response Team shall be formed that will oversee the whole operation of the BCP in its execution during actual crisis or emergency situation from the setting up of contingency or emergency operations up to the restoration to normal operations or until business operations normalize.

2. The Crisis Response Team Lead, preferably one from Senior Management, shall trigger/initiate the setting up of contingency operations when a crisis or emergency situation occurs. Based on the type of crisis situation, the Crisis Response Team shall dictate the type of contingency or emergency operations to be executed.

3. The BCP shall be tested at least annually and test results are presented to the Board.

4. An alternative/backup operations center shall be identified where personnel will be directed to proceed in a crisis or emergency situation in the event that their primary place of work is not accessible or unavailable.

5. An alternative or backup data processing site shall be available when primary data processing site is not accessible or unavailable.

6. Guidelines in the execution of contingency operations and restoration to normal operations shall be documented, tested and periodically updated. These guidelines shall include among others, resources that will be needed such as but not limited to manpower, computer systems and equipment, supplies, facilities, among others that will be used during contingency operations.

7. The contingency operations guidelines shall define the actions to be taken during crisis o emergency situations that will disrupt the bank's client services on deposits and loans processing in the head office and in the branches. Crisis or emergency situations can be categorized into:

   i. Natural calamities such as fire, extreme weather condition, flooding,
   ii. Technical problems such as power failure, system failure, communications failure,
   iii. Data security breach, and
   iv. Pandemic events such as Covid-19 virus.

8. A communications plan shall be part of the guidelines and designed to alert, notify its internal personnel that will be involved its execution of contingency operations as well as advise its clients until situation goes back to normal.