Enterprise Technology Governance & Risk Management Framework for Financial Institutions

Issued vide BPRD Circular No. 05 dated May 30, 2017

Banking Policy & Regulations Department

Table of Contents

ABBREVIATIONS/ACRONYMS

ASR	Application System Review
AUP	Acceptable Use Policy
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BoD	Board of Directors
BRD	Business Requirement Document
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information Technology
CSP	Cloud Service Provider
DFIs	Development Finance Institutions
DR	Disaster Recovery
DRP	Disaster Recovery Planning
FI(s)	Financial Institution/Institutions
HVAC	Heating, Ventilation and Air Conditioning
ICT	Information & Communication Technologies
ID	Identity (user identity)
IS	Information Systems/Information Security
ISO	International Standards Organization
ITIL	Information Technology Infrastructure Library
IT[1]	Information Technology
ITT	Invitations-To-Tender
KYC/CDD	Know Your Customer/Customer Due Diligence
MFBs	Microfinance Banks
MIS	Management Information System
PPRA	Public Procurement Regulatory Authority
RFP	Request for Proposals
RPO	Recovery Point Objective
RTO	Recovery Time Objectives
SBP	State Bank of Pakistan
SLA	Service Level Agreement
SOPs	Standard Operating Procedures
TSP	Technology Service Provider
UAT	User Acceptance Testing
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VA	Vulnerability Assessment

[1] *'IT' and 'technology' are used interchangeably in this document.*

PREAMBLE

The evolving role of technology and automation in the banking/financial services sector has become increasingly complex. A growing number of financial institutions[2] (FIs) employ the advances in technology as leverage to offer innovative products, deliver fast and efficient service at affordable prices and venture into new markets. Moreover, technology drives the efficiency of operations and financial soundness of these institutions by improving overall decision-making process. As technology becomes an integral part of the business and operations of FIs, such technology usage and dependence, if not properly managed, may heighten various risks. With a vision to provide baseline technology governance and risk management principles to the financial institutions, SBP has developed the framework on 'Enterprise Technology Governance & Risk Management in Financial Institutions'. The framework is aimed to enable FIs to keep abreast with the aggressive and widespread adoption of technology in the financial services industry and consequently strengthen existing regulatory framework for technology risk supervision. This framework shall be integrated with the FI(s)' overall enterprise risk management program. SBP expects FI(s) to have the knowledge and skills necessary to understand and effectively manage technology risks. The framework is broadly based on international standards and recognized principles of international best practices.

Purpose and Scope — The framework aims to provide enabling regulatory environment for managing risks associated with the acquisition, development, deployment and use of technology and shall serve as SBP's baseline requirements for all FI(s). The instructions are focused on enhancing the proactive and reactive environments in FI(s) to various facets and dimensions of technology including information security, technology operations, audit, business continuity, project/performance management and related domains. FI(s) shall adopt an integrated risk management approach to identify, measure, monitor and control technology risks. While implementing various aspects of this framework, FI(s) shall exercise sound judgment in determining applicable provisions relevant to their technology risk profile.

Applicability — The framework shall apply to all FI(s) which includes commercial banks (public and private sector banks), Islamic banks, Development Finance Institutions (DFIs) and Microfinance Banks (MFBs). The framework is not "one-size-fits-all" and implementation of the same need to be risk-based and commensurate with size, nature and types of products and services and complexity of technology operations of the individual FI(s). The FI(s) shall assess and conduct a gap analysis between their current status & this framework and draw a time-bound action plan to address the gaps and comply with the guidelines in this framework. The FI(s) shall upgrade their systems, controls and procedures to ensure compliance with this framework latest by **June 30, 2018.**

Status of Previous Regulatory Instructions — This framework shall supersede the following SBP instructions as issued from time to time. .

[2] Financial Institutions' refers to all banks including Commercial banks (public/private sector banks), Islamic banks, Development Finance Institutions (DFIs) and Microfinance Banks (MFBs)

- Guidelines on Information Technology Security issued vide BSD Circular No. 15 of 2004
- Guidelines on Business Continuity Planning issued vide BSD Circular No. 13 of 2004
- BCP Guidelines (Annexure – B) issued vide BSD Circular No. 03 of 2007
- Information Systems: Guidelines on Audits and System Switchover Planning issued vide BSD Circular No. 08 of 2005
- Prevention against Cyber Attacks issued vide BPRD Circular No. 07 of 2016

1. INFORMATION TECHNOLOGY GOVERNANCE IN FI(s)

Technology governance is an integral part of financial institutions (FIs)' corporate governance framework consisting of the leadership and organizational structures to ensure the alignment of IT strategy with business strategy, optimization of resources, value delivery and performance measurement to achieve business objectives and effective technology risk management. It is now recognized that technology plays a pivotal role in improving corporate governance and in this context, the need to govern technology and technology-enabled business developments have never been so greater.

A comprehensive enterprise technology governance framework based on prudent practices can help FI(s) in better development of innovative products and services by enabling them to manage technology issues and identify, measure, mitigate, monitor and report technology-based risks and threats. The underlying principle for an enterprise technology governance framework is that technology requirements of an institution follow a pre-defined process that begins with a business need and ends with a technology solution that conforms to the policies approved by the board of directors and senior management. As such, technology governance is an ongoing activity that shall not be considered a one-time effort in the fast-changing technology environment.

Technology governance aims at fully aligning technology and business strategies with each other so that technology risks are identified and controlled as part of the enterprise risk management process. It spans the culture, organizational policies and procedures which provide oversight and transparency to optimize the costs and enable trust, teamwork and confidence in the use of technology itself and the people trusted with technology services. Therefore, the processes for technology governance need to be integrated with the FI(s)' overall corporate governance framework.

1.1 Technology Governance Framework

a) The Board of Directors of the FI(s) are responsible to establish a comprehensive enterprise technology governance framework which defines the leadership, organizational structures and processes to ensure that the FI(s)' technology sustains and extends the enterprise's strategies and objectives.

b) The primary objective of the technology governance framework is to evaluate the current and future use of technology, direct the preparation and implementation of plans and policies to ensure that use of technology meets business objectives and monitor compliance to policies and performance against the plans.

c) The basic principles of strategic alignment of IT and the business, value delivery to businesses, risk management, resource management (including project management) and performance management shall form the basis of this technology governance framework.

d) Technology governance framework shall be closely aligned with FI(s)'s corporate governance framework and shall cover, among other things, policies and procedures to provide oversight and transparency in the use of technology.

e) FI(s) are encouraged to adopt relevant aspects of international standards/best practices for effective and efficient enterprise technology governance.

1.2 IT Strategy

a) The BoD shall approve "IT Strategy" covering overall design and plan of its operational framework including its vision and mission, stakeholders, business, work flow and processes, data processing, system access, adoption of best-in-class information security systems, practices and availability of IT resources.

b) The FI(s) shall identify any organizational/environmental/cultural constraints and enablers to achieve the strategic IT objectives. Further, the FI(s) shall also put in place a strategic review process to ensure that the "IT Strategy" remains relevant with the organizational strategies and direction to achieve business objectives.

1.3 Digital Strategy

The board shall also approve a "Digital Strategy" covering, at least the following objectives:-

a) Development of customer focused digital products and services.

b) End to end digitization of processes for delivery of digital products and services.

c) Interoperability of delivery channels.

1.4 Roles and Responsibilities

1.4.1 Board of Directors

The Board of Directors (BoD) sets the tone and direction for an FI(s) use of technology. BoD, at minimum, shall perform the following:-

a) Review and approve an IT governance framework to ensure that organization's IT supports and enables the achievement of the corporate strategies and objectives.

b) Review and approve "IT Strategy" and "Digital Strategy" in line with the business strategy of the bank and monitor & update the same on regular basis keeping in view potential opportunities and threats.

c) Establish an efficient and effective IT organization structure in line with the IT governance framework.

d) Ensure that technology risks are integrated with the enterprise risk management function to achieve security, reliability, resiliency, interoperability and recoverability of data/information and information assets.

e) Approve all technology-related policies and review the same periodically in light of major technological/regulatory developments at least after every three (03) years.

f) Ensure maintenance of an independent and effective technology audit function commensurate with the complexity of FI(s) technology risk profile.

g) Ensure that resource gaps (people, process & technology) identified by the management are adequately and timely fulfilled.

h) Ensure that the skills required for technology governance, service delivery, information security and risk management are sufficient and up-to-date.

i) Approve and receive periodic updates on major technology-related projects that may have significant impact on FI(s)' operations, earnings or capital. Further, the board shall also define the criteria for major projects.

1.4.2 Senior Management

The senior management, at a minimum, shall:-

a) Implement "IT strategy" and "Digital Strategy" approved by the BoD.

b) Monitor implementation of the technology governance program and assess its effectiveness on business lines and processes.

c) Implement BoD approved technology-related policies and ensure that an effective information security awareness program is implemented throughout the organization.

d) Periodically inform BoD on the latest developments on cyber security action plan its implementation status and a summary report on major threats and attacks faced by the institution and their estimated impact on its operations.

e) Ensure that the documented Standard Operating Procedures (SOPs) are in place and are effectively followed in letter and spirit in all areas of technology operations.

f) Ensure capacity building of the IT personnel to achieve desired service delivery and operational excellence.

g) Select technology solutions that can meet strategic requirements within optimum resources.

h) Ensure that an effective mechanism is in place to monitor completion of technology projects and adequate resources are available to complete these projects.

i) Identify, measure, monitor, and control the risks associated with technology-related outsourcing arrangements including cloud services.

j) Develop, conduct and maintain Disaster Recovery & Business Continuity Plans and document their testing in line with the policy approved by the board.

k) Identify resources gap (people, process & technology) and take appropriate steps to fill the gaps.

1.5 Organizational Structure

1.5.1 Board IT Committee

a) A Board IT Committee shall be constituted in all FI(s) except foreign banks, DFIs and Microfinance Banks. However, Microfinance Banks doing Branchless Banking (BB) operations shall also setup a Board IT Committee.

b) The Board IT Committee shall have a minimum of three (03) directors as its members, one of whom shall be an independent director and at least one member shall have relevant qualification or experience of IT.

c) The committee shall be mainly responsible for advising and reporting to the board on the status of technology activities and digital initiatives in the FI(s). These reports shall enable the board to make decisions without having to be involved in routine activities.

d) The committee shall review IT and Digital strategies and relevant policies before submission to the board.

e) The committee shall ensure that risk management strategies are designed and implemented to achieve resilience, such as the ability to effectively respond to wide-scale disruptions, including cyber attacks and attacks on multiple critical infrastructure sectors.

f) The committee shall receive periodic updates from IT Steering Committee to monitor all technology-related projects approved by the board.

g) The committee shall ensure that technology procurements are aligned with the IT strategy approved by the board.

h) If deem necessary, the committee may seek expert opinion from independent sources.

1.5.2 IT Steering Committee

a) The terms of reference of IT Steering Committee shall be approved by the Board IT Committee.

b) The committee shall be formulated with senior officials from different functions including IT, information security, risk management, compliance, operations and business segments.

c) The committee shall assist the senior management in implementing IT and digital strategies approved by the BoD and shall also play an advisory role to the senior management in all technology-related matters.

d) The committee shall monitor implementation of all technology-related projects.

e) The committee shall ensure that IT procurement is in line with the business plan.

f) Ensure that the outsourcing to Cloud Service Providers (CSPs) is conducted in line with the Service Level Agreement.

g) The committee shall, among other things, be responsible to ensure an efficient IT operating environment that supports the institution's goals and objectives.

h) The committee may also review and determine the adequacy of the FI(s)' training plan including information/cyber security training for the staff.

1.5.3 IT Management Structure

a) The enterprise-wide IT organizational structure shall commensurate with the size, scale, business objectives and nature of business activities carried out by the FI(s).

b) The head of information security/CISO shall be responsible for management and mitigation of information/cyber security risks across the enterprise and devising strategies to monitor and address current and emerging risks.

c) The head of information security /CISO shall be independent of the technology function to avoid any conflict of interest.

1.6 Policies, Standards and Procedures

a) The FI(s) shall formulate technology policy framework which shall be reviewed and updated at-least after every three (03) years. This framework, at a minimum, shall cover the following areas:

i) Information/cyber Security
ii) Services delivery & operations management
iii) Project management, acquisition, development & implementation of technology solutions/systems

iv) Business Continuity and Disaster Recovery

1.7 Management Information System (MIS)

a) The BoD shall put in place an appropriate MIS to oversee the implementation of IT strategy and business plan, exception from board-approved IT policies and progress on major IT projects. The format/ contents of this MIS shall be the part of policy which shall be approved by the BoD.

b) The management shall formulate an appropriate MIS to monitor the implementation of "IT governance and risk management framework". This MIS shall be the part of procedures to be approved by the management.

1.8 Capacity Building/Training

To ensure that an adequate training program is in place for IT personnel, it is essential to establish a process to identify material skill gaps of staff responsible for technology-related functions. FI(s) may encourage and where appropriate, facilitate their staff to acquire relevant professional qualifications. The FI(s) shall ensure:-

a) That hiring and training process are governed by appropriate policies and procedures.

b) That staff members have the expertise necessary to perform their jobs and achieve institutional goals & objectives.

c) Developing training programs for major new technologies before their deployment.

d) That employees are encouraged to obtain well-recognized professional certifications in order to support the business/technology objectives.

e) That staff, with privileged system access or having sensitive business functions, shall receive additional and specific information security training.

2. INFORMATION SECURITY

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

2.1 Information/Cyber Security Management Framework

An information/cyber security management framework shall be developed[3] to manage information/cyber security risks in a systematic and consistent manner. The framework, at minimum, shall include:-

a) Identification and prioritization of critical information system assets;
b) Risk management process including risk identification, risk assessment and risk treatment
c) Security controls implementation
d) Cyber security action plan to proactively address the likely cyber attacks in order to anticipate, withstand, detect, and respond to cyber attacks in line with international standards and best practices.
e) Incident reporting
f) Security requirement & testing
g) Risk monitoring & reporting
h) Threat intelligence & industry collaboration

2.2 Identification and prioritization of Information System Assets

a) FI(s) shall adequately protect critical information system assets from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

b) FI(s) shall formulate a policy on information system asset protection in which, criticality of information system assets shall be identified and ascertained in order to develop appropriate plans to protect them.

[3] If no such framework exists, FIs shall develop the same. For FIs which already have such frameworks, the same may be updated accordingly.

2.3 Information Security Risk Management

FIs shall institute the following components of risk management for the technology and infrastructure security that commensurate with size, services and complexity of the FIs operations:-

2.3.1 Risk Identification

a) FI(s) shall annually conduct a risk-based vulnerabilities identification exercise across the entire institution covering critical information systems and supporting infrastructure assets.

b) On the basis of threats and vulnerabilities, the FI(s) shall formulate a list of all risks that may create severe harm and disruption to the operations of FI(s).

2.3.2 Risk Assessment

a) After risk identification, the FI(s) shall perform an analysis and quantify the potential impact, consequences of vulnerabilities and associated risks identified in the risk identification exercise on the overall business and operations.

b) FI(s) shall develop a methodology to assess the impact of the threats to its information security environment and prioritize all material information security risks.

2.3.3 Risk Treatment

a) FI(s) shall develop and implement risk mitigation and control strategies that are consistent with the value of the information system assets and the level of risk tolerance.

b) FI(s) shall give priority to threat and vulnerability pairings with high risk ranking, which can cause significant harm or impact to the FI's operations.

c) When deciding the adoption of alternative controls and security measures, the FI(s) shall also keep in view costs and effectiveness of the controls with regard to the risks being mitigated.

d) FI(s) shall refrain from implementing and running a system where the threats to the safety and soundness of the information systems cannot be adequately controlled.

e) As a risk mitigating measure, the FI(s) may consider taking insurance cover for various insurable risks, including recovery and restoration costs.

2.4 Security Controls Implementation

2.4.1 Asset Classification and Control

The FI(s) shall maintain an inventory of all information assets and identify the information owners, who shall be responsible to ensure confidentiality, integrity and protection of these

assets. Further, the management shall implement an information classification strategy in accordance with the degree of sensitivity and criticality of information assets. Moreover, the FI(s) shall develop guidelines and definitions for each classification and define an appropriate set of controls and procedures for information protection in accordance with the classification scheme. In addition, the FI(s) shall establish secure processes for disposal and destruction of sensitive information in both paper and electronic media.

2.4.2 Physical and Environmental Protection

Physical security measures shall be in place to protect IT facilities and equipment from damage or unauthorized access. Critical information processing facilities shall be housed in secure areas such as data centers and network equipment rooms with appropriate security barriers and entry controls. Access to these areas shall be restricted to authorized personnel only and the access rights shall be reviewed and updated regularly. The FI(s) shall consider environmental threats when selecting the locations of data centers. Further, physical and environmental controls shall be implemented to monitor environmental conditions which can adversely affect the operation of information processing facilities. Moreover, FI (s) shall take adequate measures to protect equipment from power failures and electrical supply fluctuations.

2.4.3 Security Administration and Monitoring

The FI(s) shall put in place a security administration function and set formal procedures for administering the allocation of access rights to system resources and application systems and monitoring the use of system resources to detect any unusual or unauthorized activities. Further, FI(s) shall employ the "least privilege" principle throughout IT operations. Moreover, individuals with systems and security administrator roles and privileges shall have no transactional authority.

2.4.4 Authentication and Access Control

The FI(s) shall have an effective process to manage user authentication and access control. For this purpose, appropriate user authentication mechanism commensurate with the classification of information to be accessed shall be selected. Users, who can access internal systems, shall be required to accept/acknowledge an Acceptable-Use Policy (AUP) document before using a system. Staff assigned a security management function shall not perform other duties which can create any conflict of interest.

2.4.5 System Security

The FI(s) shall put in place, at a minimum, following controls and security requirements to safeguard operating systems, software and databases:-

a) Definition of a set of access privilege for different groups of users and access to data and programs.

b) Prohibition on installation of unlicensed software.

c) Installation of updated versions of software.

d) Secure configuration of hardware, operating systems, software, applications, databases and servers with all unnecessary services and programs disabled or removed.

e) Adequate documentation of all configurations and settings of operating systems, software, databases and servers.

f) Adequate logging and monitoring of systems and user activities to detect irregularities and secure protection of logs from manipulation.

2.4.6 Network Security

a) The FI(s) shall evaluate and implement appropriate controls relative to the complexity of their network. Further, the FI(s) shall deploy an effective mechanism to monitor security policy violations and atypical activities on their network.

b) The FI(s) shall consider the criticality, network protocols, performance requirements and trustworthiness in determining the network security controls appropriate to the operations of the institution and each of the security domain.

c) The FI(s) shall create backup of all device configurations on regular basis.

2.4.7 Remote Access

The FI(s) shall establish control procedures covering approval process on user requests; authentication controls for remote access to networks, host data and/or systems; protection of equipment and devices; logging and monitoring of all remote access communications and provision of more stringent security controls (i.e., data encryption, two-factor authentication process).

2.4.8 Encryption

The FI(s) shall ensure encryption at database level, storage level and during network transmission as per the classification and sensitivity of the data.

2.5 Cyber Security Action Plan[4]

The FI(s) shall formulate cyber security action plan in order to anticipate, withstand, detect and respond to cyber attacks in line with international standards and best practices.[5] The FI(s) shall implement appropriate controls to prevent any cyber security incident depending on the size and complexity of their information/cyber security environment keeping in view the following broader parameters:-

[4] This section shall supersede earlier instructions issued vide BPRD Circular No. 07of June 22, 2016 titled "Prevention against Cyber Attacks".

[5] Instructions in this section are specifically addressing external interfaces/connections of the FIs.

a) A sound governance framework with strong leadership is essential for effective enterprise-wide cyber security management. Board and senior management-level engagement along with a clear chain of accountability is critical to the success of FI(s)' cyber security action plan.

b) Developing and implementing a robust cyber security awareness program and ensuring that end-users are aware of the importance of protecting sensitive information and the risks of mishandling information.

c) The level of sophistication of technical controls employed by individual FI(s) is contingent on that FI(s) individual situation.

d) Establish written procedures to allow access to the vendors on sensitive data/information and systems.

e) Implement automated solutions to monitor and proactively track all types of cyber attacks.

f) Incorporate a consistent and comparable approach for selecting and specifying security controls for computer systems.

g) Develop and implement internal assessment methods/procedures for determining security control effectiveness.

h) Deploy multi-layer security model including firewalls, secure sign-on, dual authentication with triangulation of access and real-time security event monitoring.

2.6 Incident Reporting

a. The FI(s) shall ensure that MIS on incidents, logs, breaches etc. are regularly reviewed by the Senior Management and significant incidents are submitted for review to the IT Steering Committee on a regular basis.

b. The FI(s) shall report to Banking Policy & Regulation Department (BPRD), SBP within forty eight (48) hours after the incident[6] all established information/cyber security breaches and related incidents involving financial loss, stealing of confidential data and major disruption in the banking system or communication channel resulting in non availability of banking services for customers for more than two (02) hours

2.7 Security Requirements and Testing

a) The FI(s) shall establish a comprehensive testing program to validate the effectiveness of its information security environment on a regular basis. The results of the testing

[6] *for reporting template, refer to Annexure-I PSD Circular No. 03 of 2015 available at* http://www.sbp.org.pk/psd/2015/C3-Annexure-A.pdf

program shall be used by the FI(s) to support the improvement in their Information/cyber security. Where applicable, these tests shall include both internal and external stakeholders such as business line management, incident & crisis response teams and any other relevant departments/functions. Further, the FI(s) shall also ensure that the all production data is properly masked in the test environment involving any external party, however, for internal testing purposes, appropriate data masking may be done based on the criticality of data.

b) Keeping in view the complexities of operations, the FI(s) shall, at least employ any or combination of following testing methodologies on periodical basis, while periodicity of testing shall be defined in the policy:-

   i) **Vulnerability assessment (VA).** FI(s) shall perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes. The FI(s) shall also perform subsequent validation test to assess that the gaps identified during VA have been properly filled in.

   ii) **Scenario-based testing.** FI(s)' response, resumption and recovery plans shall be subject to periodic review and testing. Tests shall address an appropriately broad scope of scenarios, including simulation of extreme but plausible cyber attacks. Further, the tests shall be designed to challenge the assumptions of response, resumption and recovery practices including governance arrangements and communication plans. FI(s) shall also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieve strong operational resilience.

   iii) **Penetration tests.** FI(s) shall carry out periodic penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. Penetration tests on internal systems shall also be conducted at the time of major update and deployment of the software/system.

   iv) **Quality Assurance (QA).** FI(s) shall ensure that a proper and independent QA function exists and operates to testify in-house developments for any vulnerability that may pose a risk.

2.8 Risk Monitoring and Reporting

a) The FI(s) shall maintain a risk register to facilitate the monitoring and reporting of risks by prioritizing and closely monitoring high risk activities with regular reporting on the actions that have been taken to mitigate them. Further, the FI(s) shall update the risk register periodically and develop a monitoring and review process for continuous assessment and treatment of risks.[7]

[7] For this purpose, template for Risk Control & Self Assessment issued vide BPRD Circular # 04 dated May 20, 2014 available at http://www.sbp.org.pk/bprd/2014/C4-Annexure-1.pdf may be used accordingly.

b) For risk reporting to management, the FI(s) shall develop IT risk reporting methodologies to highlight systems, processes or infrastructure that have high risk exposure. In determining the IT risk reporting methodology, the FI(s) may consider risk events, regulatory requirements and audit observations.

c) The FI(s) shall evaluate the risk processes in place through testing methodologies and risk review of controls. The result of these exercises shall be duly reviewed by the management and major risks shall be reported to IT steering committee.

2.9 Threat Intelligence and Industry Collaboration

The FI(s) shall:

a) Gather and interpret information about relevant cyber threats arising out from the FI(s) participants, services and utility providers and other FI(s). In this context, relevant cyber threat intelligence may include information that may trigger cyber attacks on any entity within the FI(s)' ecosystem.

b) Ensure that cyber threat intelligence is shared with relevant staff with responsibility for the mitigation of cyber risks at the strategic, tactical and operational levels through a secure method.

c) Use a platform within the industry for the purpose of collecting and exchanging timely information that may facilitate in detection, response, resumption and recovery of FI(s) systems following a cyber attack, breach or incident.

d) Identify key lessons learnt from cyber events that have occurred within and outside the organization in order to improve their resilience capabilities and prevention mechanisms.

e) Monitor technological developments and keep abreast with new cyber risk management processes that can effectively counter existing and new forms of cyber threats.

3. IT SERVICES DELIVERY & OPERATIONS MANAGEMENT

Management shall be aware of and mitigate risks associated with technology operations. Many operations have significant risk factors that shall be addressed through effective management and control. To many FI(s), effective support and delivery from technology operations has become vital to the performance of most of their critical business lines.

3.1 IT Service Management Framework

The FI(s) shall put in place a robust IT service management framework for managing and supporting IT systems. The framework shall comprise the Preventive Maintenance Plan, Incident & Problem Management, Patch Management, Capacity Management processes and procedures for building and maintaining data centers.

3.2 Preventive Maintenance Plan (PMP)

Preventive maintenance may help in smooth and efficient functioning of IT operations, prolong the life of equipment and reduce the overall maintenance costs. Therefore, The FI(s) shall formulate preventive maintenance plan on the basis of following principles:

a) Before organizing preventive maintenance plan, FI(s) need to set goals that are to be achieved by using the system.

b) Create a list of all IT assets along with their full details.

c) Determine priority assets keeping in view the sensitivity of operations they perform. Thereafter, FI(s) shall determine that the performance of assets is in line with the operational goals.

d) Keeping in view the cost effectiveness, the FI(s) shall prioritize all IT assets, which shall be included in Preventive Maintenance Plan (PMP).

e) The FI(s) shall create a schedule for preventive maintenance plan for all the prioritized assets. Further, the IT management shall regularly review the results of the PMP.

f) The FI(s) shall focus on the capacity building of all the staff involved in the process of PMP.

3.3 Incident and Problem Management

The objective of the incident management is to restore the service as quickly as possible to meet Service Level Agreements. The process is primarily aimed at the user level. On the other hands, problem management deals with solving the underlying cause of one or more incidents. In order to have effective incident management, FI(s) shall:

a) Continuously develop problem and error controls.

b) Formulate a tiered support structure, where the team understands different levels of tiers.

c) Formulate a continual service improvement program that measures efficiency and effectiveness through KPIs aligned to organizational goals and objectives.

d) Assign clear and documented roles and responsibilities within IT in terms of desired outcomes.

For effective problem management, the FI (s) shall ensure that:-

a) The problem management process has well-defined and relevant KPIs.

b) IT function signs an internal Service Level Agreement (SLA) with business units for system availability & performance requirements, capacity for growth and level of support provided to the users.

c) Necessary arrangements are in place for backup of power supply for all areas related to IT services delivery, support and IT operations.

d) Problems and errors are regularly (and properly) classified and identified

e) Roles and responsibilities are documented in terms of desired outcomes.

3.4 Patch Management

Patch Management is a practice designed to proactively prevent the exploitation of vulnerabilities on IT devices. The FI(s) shall establish procedures to test patches in a segregated environment, and to install them when appropriate. The procedures shall include the identification, categorization, prioritization of security patches and their testing processes.

3.5 Capacity Planning

a) The FI(s) shall initiate capacity planning to address internal factors (growth, mergers, acquisitions, new product lines and the implementation of new technologies) and external factors (shift in customer preferences, competitor capability or regulatory or market requirements).

b) The FI(s) shall monitor technology resources for capacity planning including platform processing speed, core storage for each platform's central processing unit, data storage, and voice/data communication bandwidth.

c) Capacity planning shall be closely integrated with the budgeting and strategic planning processes. It shall also address personnel issues including staff size, appropriate training and staff succession plans.

3.6 Data Center

The FI(s) shall formulate procedures in line with best international standards for building and maintaining data center structures and operations.

3.7 User Support/Help Desk

The FI(s) may create users' help desk to ensure that they perform their job functions in an efficient and effective manner. The Help Desk may record and track incoming problem reports, being handled by live operators or automated systems. Further, FI(s) may also define Key performance indicators (KPI) for the resolution of different problems / issues.

4. ACQUISITION & IMPLEMENTATION OF IT SYSTEMS

The critical role of technology in financial institutions requires the use of appropriate development, acquisition and maintenance standards. Development and acquisition refers to an organization's ability to identify, acquire, install and maintain appropriate information technology systems. The process includes the internal development of software applications or systems and the purchase or acquisition of hardware, software, or services from third parties. The development, acquisition and maintenance process includes numerous risks. Effective project management manages the possibility of loss resulting from inadequate processes, personnel or systems. Losses can result from errors, fraud or an inability to deliver products or services, maintain a competitive position or manage information.

4.1. Technology Projects Management Framework

The FI(s) shall:

a) Establish a framework for management of major technology-related projects. This framework shall, among other things, specify the project management methodology to be adopted. The methodology shall at a minimum cover structure, roles and responsibilities of the staff, activity breakdown, budgeting of time and resources, milestones, check points, key dependencies, quality assurance, change management, risk assessment and approvals.

b) Establish a Project Management Office (PMO) to promote sound management practices and principles based on the size and complexity of technology-related projects. Further, PMO shall be responsible to maintain centralized record of all technology related projects, monitor and report the status of these projects to the IT steering committee on periodical basis.

c) Adopt and implement a full project life cycle methodology governing the process of developing, implementing and maintaining major computer systems. In general, this shall involve phases of project initiation, feasibility study, business requirement definition, system design, program development, system and acceptance testing, training, implementation, operation and maintenance. The project life cycle methodology shall include roles and responsibilities for the project team and the deliverables from each phase.

d) Engage an independent party to conduct a quality assurance review of major technology projects after every five (05) years.

4.2 System Development and Acquisition Framework

The FI(s) shall assess and mitigate operational risks associated with the development or acquisition of software by using a Secure System Development Life Cycle (SDLC) or similar methodology appropriate for their specific technology environment. The extent or use of the

SDLC shall depend on the size and complexity of the institution and the type of development activities performed.

The system development and acquisition framework shall at least cover the following aspects:-

4.2.1 System Development

Software development projects can be completed by the FI in-house, through outsourcing or by a combined approach. To manage such type of projects, the FI(s) shall ensure that:

a) Project management standards are in place to address issues such as need assessment, risk management procedures and project approval authorities.

b) System control standards include an application's functional, security, and automated control features.

c) Quality assurance standards address issues such as validation of project assumptions, adherence to project standards and testing of a product's performance.

d) Security and vulnerability assessment of software modules is conducted.

e) An escrow arrangement exists in cases where core applications are developed by vendors but the source codes were not released to the FI(s).

4.2.2 System Acquisition

a) For major IT acquisitions, FI(s) shall develop/update technology procurement policy covering, at least, the following areas:-

   i) Formulation of RFP and Business Requirement Document (BRD)

   ii) Roles and responsibilities of relevant stakeholders

   iii) Approval matrix of RFP and BRD

b) The technology procurement policy shall also include types of technology assets for both hardware & software, types of vendors for hardware & software, selection criteria for vendors, acquisition process, payment procedures & monitoring, delivery assurance & verification process, technical vetting requirement and need assessment.

c) The FI(s) shall ensure that functional, operational and regulatory requirements are identified and recorded in Request-For-Proposals (RFP) or Invitations-To-Tender (ITT) in the bid solicitation process. Public sector FI(s) shall also follow PPRA rules for procurement of any software or hardware solutions or consultancy services.

d) The RFP and BRD for any new technology acquisition shall be reviewed to ascertain comprehensiveness of the documents, their alignment with IT strategy & business objectives and technical alignments with emerging trends and technologies.

e) FI(s) may obtain expert consultancy/ advisory services for the formulation of RFP/BRD/Procurement process, where it deems necessary, provided they record reasons and rationale for the same.

f) FI(s) shall conduct a system (hardware, software and services) selection analysis to ensure that user and business requirements are met, expected service levels are properly achieved as per contract agreements and all applicable legal/regulatory requirements are complied with.

g) FI(s) shall undergo a transparent and competitive process of acquisitions in major procurements. Whenever signing up for direct contracting is required, it should be fairly justified based on the requirements (such as technical grounds, urgency and other matters).

h) The procurement process shall b e managed by an independent unit and governed by IT Steering Committee for different scope / level / size of procurements.

i) FI(s) shall form an appropriate forum/structure to monitor the process of technology related procurements.

j) FI(s) shall also ensure that vendors deliver hardware/ software as per terms and conditions set in the contract/agreement. The delivery of technology assets shall be assessed against purchase orders, prepared in light of RFPs/ BRDs, and the same shall be signed off by the respective departments.

4.2.3 System Testing

The FI(s) shall:

a) Ensure that only properly tested and approved systems are promoted to the production environment.

b) Carry out system and User Acceptance Testing (UAT) in an environment separate from the production environment.

c) Ensure that production data is not used in development or acceptance testing unless the data has been desensitized and prior approval from the information owner has been obtained.

d) Carry out performance testing of newly developed critical systems to ensure effective and smooth operation before deploying the same in production environment.

e) Conduct system testing using documented test plans encompassing all predetermined data or processing problems and business scenarios.

f) Ensure that adequate test scenarios are formulated and sufficiently tested in UAT.

g) Confirm that test activities are successful and recorded before the modified programs is transferred to the production environment.

h) Ensure that system development personnel are prohibited from having access to production systems.

4.2.4 System Migration

The FI(s) shall:

a) Establish a secured library or quarantine area for program pending migration to the production environment, which are accessible by the personnel, who have performed the migration process.

b) Put in place an appropriate procedure to verify changes and to ensure that no unauthorized changes have been made.

c) Implement version controls to ensure that only authorized programs are migrated to quarantine and production environments.

d) Archive old versions of source codes with a clear indication of the precise date, time and all necessary information.

4.2.5 System Documentation

The FI(s) shall:

a) Formulate procedures on system development and all related documentation including development, testing, trainings, production, operational administration and user manuals.

b) Maintain the type and level of documentation for each project phase including project requests, feasibility studies, project plans, testing plans etc.

c) Establish system documentation including system concept narratives, data flow charts and database specifications.

d) Establish application documentation including application descriptions, programming flowcharts, work flow processes, operations and user instructions.

e) Define roles and responsibilities of officers to ensure that all changes to system, application and configuration documentation are made according to prescribed standards.

f) Control access to documentation libraries with appropriate library and version controls.

g) Ensure that complete and updated system documentation of such applications is available and are secured against unauthorized access.

4.2.6 Change Management

a) FI(s) shall establish a change management process to ensure that changes to production systems are approved, implemented and reviewed in a controlled manner.

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

c) FI(s) shall perform a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems.

d) FI(s) shall adequately test the impending change and ensure that it is accepted by users prior to the migration of the changed modules to the production system. The FI(s) shall develop and document appropriate test plans for the impending change. Further, they shall obtain test results with user sign-offs prior to the migration.

e) FI(s) shall establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. The FI(s) shall establish alternative recovery options to address situations where a change does not allow the FI to revert to a prior status.

f) FI(s) shall ensure that the logging facility is enabled to record activities that are performed during the migration process.

4.2.7 Post-Implementation Review

For critical projects/systems, the FI(s) shall:

a) Conduct a post implementation review at the end of a project to validate the application's operational performance.

b) Assess the relative success of the project by comparing planned and actual cost, benefits and completion time.

c) Record reasons in a post implementation evaluation report if the planned objectives do not materialize.

d) Present post implementation evaluation report to senior management highlighting operational or project management deficiencies (if any).

4.3 Outsourcing of IT Services

The FI(s) shall define the business requirements for the functions or activities to be outsourced. All IT activities to be outsourced shall be governed under the instructions conveyed through BP&RD Circular No 9 dated 13th July, 2007 as amended from time to time.

4.4 Cloud Computing

4.4.1 Due Diligence of the Cloud Service Provider (CSP)

When evaluating the feasibility of outsourcing to a CSP, FI(s) shall keep in view the legal, regulatory & compliance risks, cost effectiveness and quality of services etc. Further, FI(s) shall carry out due-diligence of the prospective CSPs including their competence, business structure, experience, track record, financial strength, physical security/internal controls placed by the CSP.

The board shall formulate a comprehensive policy on due-diligence and risk management of CSP based on the following parameters before allowing services on cloud:-

a) **Data ownership**: The FI (s) shall be ultimate responsible for the security of the data.
b) **Data Separation/Isolation**: FI's data must be segregated from other data held by the CSP.
c) **Security, Privacy & Confidentiality**: The CSP or any other entity shall not have the right to view or access the information being routed or stored with the CSP. The sole discretion of access to all such information/data/records/reports etc shall be with the FI(s).
d) **Audit & Access Rights**: A CSP shall provide access of all arrangements to FI(s) and SBP.
e) **Review, Monitoring and Control**: A CSP shall demonstrate compliance with all legal and contractual requirements.
f) **Encryption and Key Management**: FI(s) confidential or sensitive data must be appropriately protected. Keys used for appropriate encryption adopted by the FI(s) shall be managed securely.
g) **Service Legal Agreement (SLA)**: All arrangements shall be properly documented in the SLA between the CSP and the FI(s).
h) **Business Continuity Plan**: FI(s) shall have adequate plan to resume business due to any disruption of services through CSP.

i) **Exit Strategy**: FI (s) shall put in place adequate procedures to exit from the cloud computing arrangement in case of non compliance of terms and condition of the agreement by CSP. These shall also be made the part of agreement with CSP.

4.4.2 Permissible Cloud Computing Arrangements

The Board IT Committee shall approve all cloud-based outsourcing arrangements in line with the policy approved by the board keeping in view the following:-

a) Given the potential issues related to business operations, confidentiality of customer data and legal/regulatory compliance, FI(s) shall only use cloud services for non-core operations and business support processes (e.g., communication tools, office productivity, collaboration tools, HR-related services, procurement functions, Inventory management etc.)

b) For all types of cloud services including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), the CSPs shall be located in Pakistan and all physical servers and services (data centers and allied infrastructure) shall reside and operate from Pakistan.

c) Core banking applications/services/operations and business processes used to process and store customer/borrower data/information shall not be placed under cloud-based outsourcing arrangements.

5. BUSINESS CONTINUITY AND DISASTER RECOVERY

Financial institutions could face the suspension of critical operations due to natural disasters, terrorist attacks, environmental incidents, computer problems, and other causes and hence need to secure business continuity by formulating action plans in advance to ensure quick recovery. Business Continuity Planning (BCP) is a comprehensive enterprise-wide process that defines how FI(s) respond to and recover from business disruptions in case of a disaster, enabling an FI(s) to continue services to the customers and stakeholders alike.

5.1. Business Continuity and Disaster Recovery Framework

a) The FI(s) shall develop a comprehensive business continuity plan (BCP) as part of the business continuity planning process.

b) The BCP shall be based on the size and complexity of the FI(s) and shall be consistent with its overall business strategy.

c) The goal of the BCP shall be to minimize financial losses to the institution, serve customers with minimal disruptions and mitigate the negative effects of disruptions on business operations.

d) Keeping in view the size, nature and complexity of business operations and IT systems, FI(s) shall consider developing built-in redundancies to reduce single points of failure which can bring down the entire network.

e) The FI(s) shall maintain standby hardware, software and network components that are necessary for fast recovery.

5.2 Business Continuity Planning Process

Business continuity planning process includes a Business Impact Analysis (BIA), risk assessment, risk management, risk monitoring and testing.

5.2.1 Business Impact Analysis

The FI(s) shall:

a) Assess and prioritize all business functions and processes, including their interdependencies, as part of a work flow analysis,

b) Identify potential impact of business disruptions resulting from uncontrolled, non-specific events on the institution's business functions and processes,

c) Identify legal and regulatory requirements for the FI(s) business functions and processes,

d) Estimate maximum allowable downtime as well as the acceptable level of losses, associated with business functions and processes and

e) Estimate recovery time objectives (RTOs), recovery point objectives (RPOs) and recovery of the critical path.

5.2.2 Risk Assessment

The FI(s) shall:

a) Evaluate the BIA assumptions using various threat scenarios;

b) Analyze threats based upon the impact to the institution, its customers and other relevant stakeholders;

c) Prioritize potential business disruptions based on their severity; and

d) Perform a "gap analysis" to compare existing BCP to the policies and procedures which shall be implemented based on prioritized disruptions identified and their resulting impact on the FI(s).

5.2.3. Risk Management

Risk management is the process of identifying, assessing, and reducing risk to an acceptable level through the development, implementation and maintenance of a written, enterprise-wide BCP. The BCP shall be based on a comprehensive BIA and risk assessment exercise, reviewed and approved by the board at least annually. It shall be documented in a written program and disseminated across the FI(s). The BCP shall, among other things, specify the conditions which shall prompt implementation of the plan and the process for invoking the BCP and immediate steps to be taken during a disruption. The BCP shall be flexible to respond to unanticipated threat scenarios and changing internal conditions; focused on the impact of various threats that could potentially disrupt operations rather than on specific events; BCP shall be effective in minimizing service disruptions and financial loss through the implementation of mitigation strategies.

5.2.4. Risk Monitoring and Testing

Risk monitoring and testing is the final step in the business continuity planning process. Risk monitoring and testing ensures that the institution's business continuity planning process remains viable through the:

a) Incorporation of the BIA and risk assessment into the BCP and testing program;

b) Development of an enterprise-wide testing program;

c) Assignment of roles and responsibilities for implementation of the testing program;

d) Completion of annual, or more frequent, tests of the BCP;

e) Evaluation of the testing program and the test results by senior management and the board;

f) Assessment of the testing program and test results by an independent party; and

g) Revision of the BCP and testing program based upon changes in business operations, audit recommendations and test results.

5.3 Disaster Recovery

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

5.3.1. Disaster Recovery Plan

The FI(s) shall:

a) Identify and address various types of contingency scenarios, which may be caused by system faults, hardware malfunction, operating errors or security incidents and total incapacitation of the primary Datacenter.

b) Evaluate the recovery plan and incident response procedures at least annually and update them as and when changes to business operations, systems and networks occur.

c) Implement replication, rapid backup and recovery capabilities at the individual system or application cluster level.

d) Consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.

e) Define system recovery, business resumption priorities and establish specific recovery objectives including Recovery Time Objectives (RTO) and Recovery Point Objective (RPO) for IT systems and applications.

f) Establish a recovery site that is geographically separated from the primary site to enable the restoration of critical systems and resumption of business operations in case of disruption at the primary site. Further, FI (s) shall also address cross-border network redundancies (in case of offshore outsourcing arrangements), with strategies such as engagement of different network service providers and alternate network paths.

g) The selection of DR specifications shall be made according to the BIA to address the identified threats and to meet the recovery objectives.

5.3.2 Disaster Recovery Testing

1. The FI(s) shall:
   a) Adopt approved, tested and rehearsed recovery measures.

   b) Test and validate, at least annually, the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

   c) Cover various scenarios in disaster recovery tests including total shutdown/complete switchover of the primary site as well as component failure at the individual system or application cluster level.

   d) Test the recovery dependencies between systems.

   e) BCP/DR drills planned with third parties, if any, shall be performed annually.

   f) Testing of BCP shall include all aspects and constituents of a bank i.e. people, processes and resources (including technology). BCP tests shall ensure that all members of the recovery team and relevant staff are aware of the plans.

   g) Involve business users in the design and execution of comprehensive test cases to verify that recovered systems function properly.

   h) Participate in disaster recovery tests that are conducted by its service provider(s), including those systems, which are located offshore.

   i) Involve the respective business group heads/ unit heads while signing-off test results of DR-BCP drills.

6. IT AUDIT

The FI(s) shall plan, manage and monitor rapidly changing technologies to enable them to deliver and support new products, services and delivery channels. These changes and the increasing reliance on technology make the IT audit coverage essential to an effective overall audit program. The audit program shall address technology risks throughout the organization, including the areas of IT management, strategic planning, IT operations, physical and information security, electronic products and services, systems development & acquisition and business continuity planning etc.

6.1. IT Audit Program

The audit function of FI(s) shall ensure that an audit program, governing the IT audit function, is approved by the BoD or its Audit Committee, which shall at a minimum, include the following:-

a) An annual audit plan detailing IT audit's budgeting and planning processes including audit goals, schedules, staffing needs and reporting requirements.
b) A risk assessment process to describe and analyze the risks inherent in a given line of business for the determination of scope and frequency of audits.
c) An IT audit cycle that identifies the frequency of audits based on sound risk assessment process;
d) Audit report format;
e) Document maintenance and retention policy for IT findings.
f) Follow-up processes for significant IT audit findings.

6.2 Scope of IT Audit

The scope of IT audit shall include:-

a) Identification of weaknesses, providing meaningful recommendations and reviewing management's plans for addressing those weaknesses.

b) Reviewing the adequacy of general controls in place covering areas such as IT strategic & business planning, IT operations, DR/BCP, IT outsourcing, information security, development and acquisitions, ADCs, IT Procurements and Project Management etc.

c) A regular, comprehensive audit of FI(s) arrangements with the CSPs.

d) Application System Review (ASR) to identify, document, test and evaluate the application controls to ensure confidentiality, integrity and accuracy of the systems and the related data/information.

6.3 Reporting Methodology

The audit function shall:

a) Report the findings, conclusions, recommendations and qualifications or limitations in scope with respect to the IT audit.

b) Discuss the draft report contents with management in the subject area prior to finalization and release of the final report.

c) Ensure that report is signed, dated and distributed according to the format as defined in the audit program.

d) Periodically submit a consolidated report to the Audit Committee on the following areas:-
    a. Information/cyber security
    b. IT service delivery and operations
    c. IT outsourcing including cloud services arrangements
    d. IT Project management, acquisition & development
    e. IT procurement
    f. Performance Management
    g. BCP & DRP

6.4 Post-closing/Monitoring Activities

a) The audit function shall ensure that senior management approves a procedure to ensure timely implementation of audit recommendations.

b) The audit function shall monitor the implementation of management's corrective actions.

c) The audit function shall communicate status of the recommendations to the BoD or Audit Committee at least on a quarterly basis.