Framework on Information Technology Governance & Risk Management in Financial Institutions

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
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
IT	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

PREAMBLE

The evolving role of technology and automation in the banking/financial services sector has become increasingly complex. A growing number of financial institutions[1] (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 technology risks. With a vision to provide baseline technology governance and risk management principles to the financial institutions, SBP has developed the framework on 'Information Technology Governance & Risk Management in Financial Institutions' to keep abreast with the aggressive and widespread adoption of technology in the financial service industry and consequently strengthen existing regulatory framework for IT risk supervision. The framework is broadly based on COBIT framework. This framework shall be integrated with the financial institutions' overall enterprise risk management program. SBP expects FIs to have the knowledge and skills necessary to understand and effectively manage technology risks. These institutions are required to have an integrated approach to risk management to identify, measure, monitor and control risks.

Purpose and Scope — The framework aims to provide enabling regulatory environment for managing risks associated with use of technology. The framework is based on international standards and recognized principles of international practice for technology governance and risk management and shall serve as SBP's baseline requirement for all FIs. The FIs shall ensure compliance with this framework while introducing new products either all by themselves; or in the form of co-branding or in partnership with other entities

Applicability — The framework shall apply to all FIs 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 IT operations of the individual FIs. The instructions are focused on enhancing the proactive and reactive environments in FIs to various facets and dimensions of the information technology, security, operations, audit and related domains and to create overall safe and secure technology operations in FIs which will benefit and enhance the confidence of all the stakeholders. The FIs are expected to assess and conduct a gap analysis between their current status and the guidelines and draw a time-bound action plan to address the gaps and comply with the guidelines. FIs shall exercise sound judgment in determining applicable provisions relevant to their risk profile. The FIs shall upgrade their systems, controls and procedures to ensure compliance with these instructions latest by December 31, 2017.

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

1. INFORMATION TECHNOLOGY GOVERNANCE IN BANKS

Information Technology (IT) 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 resource, IT value delivery and performance measurement to achieve business objectives and effective IT risk management implementation. It is now recognized that IT plays a pivotal role in improving corporate governance and in this context, the need to govern IT and IT enabled business developments have never been so greater.

An enterprise IT Governance Framework is the overall design and high-level plan that defines an institution's operational framework and includes the institution's mission, stakeholders, business and customers, work flow and processes, data processing, system access and its security. A comprehensive enterprise IT Governance Framework based on prudent practices can help FI(s) in better development of innovative product and services by enabling them to manage IT issues and identify, measure, mitigate, monitor and report technology-based risks and threats. The underlying principle for an enterprise IT Governance Framework is that IT requirements of an institution follow a pre-defined process that begins with a business need and ends with an IT solution that conforms to the policies approved by senior management and the board of directors. As such, IT Governance is an ongoing activity that should not be considered as a onetime effort in the fast changing IT environment.

IT Governance primarily focuses that the IT function of the organizations are fully aligned to the business strategies and direction, key risks are identified & controlled and legislative and regulatory compliance are in place to mitigate the risks. IT Governance spans the culture and organizational policies & procedures that not only provide oversight and transparency to optimize the cost but also engender greater trust, teamwork and confidence in the use of IT itself and the people trusted with IT services. Therefore, the processes for IT Governance need to be integrated with the Corporate Governance.

1.1 IT Governance Framework

A comprehensive enterprise IT Governance Framework shall enable an FI to evaluate the current and future use of IT, direct the preparation and implementation of plans and policies to ensure that use of IT meets business objectives and monitor conformance to policies, and performance against the plans. IT Governance framework entails an IT strategy, organizational structures, roles of the board and senior management and IT policy framework. Broadly an enterprise IT Governance Framework of an FI shall aim to achieve the following institutional objectives:

a) Strategic Alignment – Alignment of the strategic direction of IT with the business with respect to services & projects and verifying strategic compliance, i.e. achievement of organizational objectives through strategic IT objectives.

b) Value Delivery – Ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs & proving the intrinsic value of IT.

c) IT Risk Management – Ensuring that processes are in place and effective to assess and manage the associated risks in IT investments, developments and operations.

d) Optimal Resource Management – Ensuring that there is an adequate IT capability and infrastructure to support current and expected future business requirements.

e) Performance Management - Reviewing the measurement of IT performance and the contribution of IT to the business (i.e. delivery of promised business value).

f) Adequate IT Policy Framework – ensure that the appropriate policy controls are in place and the processes are standardized and documented.

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, security, and availability of IT resources. An effective IT strategy shall ensure delivery of IT services that balance cost and efficiency, while enabling the business units to meet the competitive demands of the marketplace. IT strategy's key components shall at minimum include information security, business resilience, data management, external connectivity, and alignment with FI's goals and objectives.

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. The FI(s) IT strategy shall aim to achieve, among other, the following objectives

i) Enhanced interoperability from using IT to drive business adaptability.

ii) Closer partnership between business and IT groups.

iii) Improved focus on the institution's goals.

iv) Reduced complexity of IT systems.

v) Improved agility of IT systems.

vi) Closer alignment between IT deliverables and business requirements.

vii) Compliance with legal and regulatory requirements

1.3 Roles and Responsibilities

1.3.1 Board of Directors

IT Governance needs a mandate and direction from Board, therefore the Board of Directors (BoD), at a minimum, shall:-

a) Approve overall Enterprise IT strategy in line with the business strategy of the bank and monitor & update the same on regular basis keeping in view upcoming opportunities and threats.

b) Approve an IT governance framework to ensure that organization's IT infrastructure supports and enables the achievement of the corporate strategies and objectives.

c) Ensure that effective IT risk management and internal controls functions are in place to achieve security, reliability, resiliency, interoperability and recoverability.

d) Approve all IT Management and Information/cyber Security policies and review report on the effectiveness of the information security program at least on annual basis.

e) Oversee a safe, sound, controlled and efficient IT operating environment that supports the institution's goals and objectives.

f) Review, approve, and monitor IT projects that may have significant impact on FIs' operations, earnings or capital.

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

h) Review and approve the IT related policies including Disaster Recovery and Business Continuity plans in line with the best international practices and standards. that are appropriate for the size and complexity of the organization

i) Ensure resources gap (people, process & technology) identified by the management are adequately and timely fulfilled.

1.3.2 Senior Management

The senior management, at a minimum, shall:-

a) Implement the IT strategy approved by the BoD.

b) Establish an efficient and effective IT organization structure and approve job descriptions of all IT officials.

c) Ensure implementation of IT risk management and internal control functions to achieve security, reliability, resilience and recoverability.

d) Implement BoD approved IT Management and Information Security Policies and ensure that an effective information security awareness program is implemented throughout the organization.

e) Ensure that FI’s risk management policy incorporates IT-related risks, which shall be reviewed and updated on periodical basis.

f) Monitor implementation of the IT Governance program and assess its effectiveness on business lines and processes.

g) 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.

h) 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 possible impact on its operations on periodical basis.

i) Ensure that the documented Standard Operating Procedures are in place and are effectively followed in letter and spirit in all areas of IT Operations.

j) Ensure that FI(s)'s physical infrastructure is adequate to accomplish the strategic plans of the organization.

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

l) Select IT solutions that can meet strategic requirements with minimum resources.

m) Ensure that IT projects support business objectives and adequate resources are available to complete these projects.

n) Ensure that risks related to IT projects are appropriately managed.

o) Ensure that an effective monitoring mechanism is in place to evaluate the design of IT projects and oversee the related operations and activities.

p) Monitor implementation of outsourcing process to identify, measure, monitor, and control the risks associated with IT-related outsourcing arrangements.

q) Develop, conduct, document and maintain BCP and the testing program.

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

1.4 Organizational Structure

1.4.1 Board IT Committee

a) The Board IT Committee shall be set up with a minimum of three directors as its members, one of whom shall be an independent director and at least one member shall have qualification or experience of holding key IT positions. The committee shall report to the board of directors.

b) The committee shall be mainly responsible for reporting to the board on the status of IT activities. The reports enable the board to make decisions without having to be involved in routine activities.

c) The committee shall be responsible for formulation of IT strategy and IT policy framework, review and implementation of IT strategy and policy framework, guiding the management for necessary course of action, oversight of IT performance and aligning IT with business needs.

d) The committee shall receive appropriate information from IT, lines of business, and external sources. Additionally, it shall coordinate and monitor the institution's IT resources.

e) The committee may also review and determine the adequacy of the institution's training plan including cyber security training, for the staff.

1.4.2 IT Steering Committee

a) IT Steering Committee of the management shall be formulated with members from different functions including IT, IT security, risk management, compliance, operations and business segments.

b) The committee shall assist the senior management in implementing IT strategy approved by the BoD and shall also play an advisory role to the senior management in all IT related matters.

c) The scope of the committee may include strategic IT planning, risk treatment, oversight of IT performance, and aligning IT with business needs. The steering committee shall have a charter that defines its responsibilities.

d) If deem necessary, the committee may seek expert opinion in matters from an independent source.

1.4.3 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). The Chief Risk Officer shall be responsible to review, asses and manage IT related risks

b) The structure shall consist of leading and responsible roles such as Chief Information Officer (CIO)/Head of IT, Chief Technology Officers, Chief Information Security Officer (CISO)/Head of IS/IT security etc.

c) The head of information security function may report directly to Chief Risk Officer of the FI.

1.5 IT Policies, Standards, and Procedures

a) Given the criticality of the IT, FI(s) may follow relevant aspects of such standards that have found acceptability in the industry including but not limited to COBIT 5 framework etc.

b) The FI(s) shall formulate IT policy framework which shall be reviewed and updated 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 IT Systems
iv) Business Continuity and Disaster Recovery

1.6 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 of board approved IT policies and progress of major IT projects. The format/ contents of this MIS shall be the part of policy which will be approved by the BoD.

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

1.7 Capacity Building/Training

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 and objectives.

c) Developing training programs for new technologies and products before their deployment. The FI(s) shall encourage employees to obtain an external certification to ensure that they maintain the necessary expertise to support the business objectives.

d) That staff, with privileged system access or having sensitive business functions, shall receive targeted 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, and availability and durability of IT resources and their associated 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 IT risk profile. Management may consider a variety of policies, procedures, and 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 to manage IT risks in a systematic and consistent manner. The framework, at minimum, shall include:-

a) Identification and prioritization of information system assets;
b) Risk Management Process including risk assessment, risk identification, and risk treatment
c) Security Control Implementation
d) Cyber security action plan 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 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.

2.3 Risk Management Process

2.3.1 Risk Identification

a) FI(s) shall determine threats and vulnerabilities to its IT environment, which comprises the internal and external networks, hardware, software, applications, databases, systems interfaces, operations, data centers and human elements.

b) FIs shall execute quarterly software's vulnerabilities identification operation across the entire institution covering all IT systems and supporting infrastructure assets (Networks, PCs, Laptops, servers, operating systems, software, applications, and databases)

c) 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 quantification of the potential impact and consequences of identified and unidentified vulnerabilities and associated risks on the overall business and operations.

b) FI(s) shall develop a threat and vulnerability matrix to assess the impact of the threat to its IT environment, which will also assist the FI(s) in prioritizing IT 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) FI(s) shall assess its risk tolerance for damages and losses in the event that a given risk-related event materializes.

d) 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.

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

f) 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 in ensuring 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 ensure that all media are adequately protected and 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 should be reviewed and updated regularly. The FI(s) shall consider the environmental threats when selecting the locations of its 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 interferences.

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 minimal 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 sign an Acceptable-Use Policy (AUP) document before using a system. Further, the FI(s) shall implement effective password rules to ensure that easy-to-guess passwords are avoided and passwords are changed on a periodic basis.

2.4.5 System Security

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

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

b) Prohibition of installation of Unlicensed Software.

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

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

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

2.4.6 Network Security

1) 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 cross-domain access for security policy violations and anomalous activities.

2) 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 domains.

3) The FI(s) shall create backup of all device configuration 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 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/ transport for critical/confidential data.

2.5 Cyber Security Action Plan

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. The FI(s) shall implement appropriate controls to prevent any cyber security incident depending on the size and complexity of its IT environment keeping in view the following broader parameters:-

a) A sound governance framework with strong leadership is essential to effective enterprise-wide cyber security. Board-level and senior management-level engagement is critical to the success of firms' cyber security programs, along with a clear chain of accountability.

b) Establishing and maintaining a robust and properly implemented 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 an individual FI is contingent on that FI's individual situation. While a smaller institution may not be positioned to implement the included controls in their entirety, but these strategies can serve a critical benchmarking function to support an understanding of vulnerabilities relative to industry standards.

d) FI (s) use third-party vendors for services, which requires vendor access to sensitive information, or access to firm systems. The FI (s) shall manage cyber security risk exposures that arise from these relationships by exercising strong due diligence and developing clear performance and verification policies.

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

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

g) Creating a foundation for the development of internal assessment methods and procedures for determining security control effectiveness.

h) Ensure to 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. shall be submitted for review to the IT Steering Committee on a regular basis.

b. The FI(s) shall report all IT related incidents involving financial loss to the institution, stealing of confidential data and non availability of banking services for customers for more than 2 hours to Banking Policy & Regulation Department, SBP within forty eight (48) hours after the incident. (*for reporting template, refer to Annexure-I PSD Circular No. 03 of 2015*)

2.7 Security Requirements and Testing

a) The FI(s) shall establish a comprehensive testing program to validate the effectiveness of its IT environment on a regular basis. The results of the testing program shall be used by the FI(s) to support the improvement of their IS/cyber security. Where applicable, these tests shall include both internal and external stakeholders such as business line management, incident & crisis response teams and players of relevant entities in the ecosystem. Further, the FI(s) shall also ensure that the production data is properly masked in the test environment.

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

FIs 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. FIs shall also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving strong operational resilience.

iii) **Penetration tests.** FI(s) shall carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of FIs' systems, these tests shall simulate actual attacks on the systems. Penetration tests on internet-facing systems shall also be conducted at the time of update and deployment of systems. Where applicable, the tests may include other internal and external stakeholders, such as those involved in business continuity, incident and crisis response teams as well as third parties service providers.

iv) **Quality Assurance (QA).** FI(s) shall ensure that a proper and independent QA function exists and operate 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 institute a monitoring and review process for continuous assessment and treatment of risks.

b) For risk reporting to management, the FI(s) shall develop IT risk metrics to highlight systems, processes or infrastructure that have high risk exposure. In determining the IT risk metrics, 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 put up to IT steering committee as per TORs of the 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, service and utility providers and other FIs. 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) Shall identify key lessons learnt from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities and prevention.

e) Shall monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber attack.

3. IT SERVICES DELIVERY & OPERATIONS MANAGEMENT

Management shall be aware of and mitigate risks associated with IT operations. The FI and its service providers may have one or more IT operations groups. Common examples of IT operations are data center or computer operations, network services, distributed computing, personal or desktop computing, change management, project management, security, resource management, and contingency and resiliency planning.

Many operations functions have significant risk factors that shall be addressed through effective management and control. To many FI(s), effective support and delivery from IT 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, Event & Problem Management, Patch Management process, capacity management procedures and procedures for building and maintaining data centers.

3.2 Preventive Maintenance Plan (PMP)

Preventive maintenance may keep IT operation running smoothly and efficiently, 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 Management 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 Event and Problem Management

The objective of the Incident Management Lifecycle 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 its testing process.

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 and 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. This help 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 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. IT Project Management Framework

The FI(s) shall:

a) The FI(s) shall: 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 of 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 their IT projects. The PMO shall be responsible to monitor, review and report the status of various IT projects to the IT steering committee on quarterly basis. Further, project status summaries shall be submitted to the Board on bi-annual basis.

c) Engage an independent party to conduct a quality assurance review of major IT-related projects after every three (03) years.

4.1.1 IT Project Planning and Initiation

The FI(s) shall:

a) Identify the expected costs and benefits of developing a system, and also to decide either to utilize internal resources or to outsource the same to a vendor.

b) 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.

4.1.2. Change Management

a) FI(s) shall establish a change management process to ensure that changes to production systems are assessed, 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 Software Development and Acquisition Framework

The FI(s) shall assess and mitigate operational risks associated with the development or acquisition of software by using a System Development Life Cycle (SDLC) or similar methodology appropriate for the specific IT environment. The extent or use of the SDLC depends on the size and complexity of the institution and the type of development activities performed. If the FI(s) primarily acquire(s) software, management shall verify the effective use of an SDLC by the third-party provider. Broadly, the system development and acquisition framework shall at least cover the following aspects:

4.2.1 Systems Development

Software development projects can be completed 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.

4.2.3 System Acquisition

a) The FI(s) shall formulate IT 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 IT Procurement Policy shall also include types of IT 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 RFP and BRD for any new IT 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.

d) FI(s) may engage consultant/ advisor for the formulation of RFP/BRD/Procurement Process, where it deems necessary, provided the FI records reasons and rationale for the same.

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

f) 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).

g) The procurement process shall be managed by an independent unit and governed under high level committees for different scope / level / size of procurements.

h) FI(s) shall preferably form an IT Procurement Committee to ensure that requirements of IT procurement policy are complied with in letter & spirit. The committee may include members from IT, business, Finance/ Accounts and general services/ administration division/ departments.

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

4.2.4 Systems 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 before newly developed systems are migrated to the 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.

4.2.5. Systems 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 source compare procedure to verify changes and to ensure that no unauthorized changes have been made.

c) Compare modified programs to the authorized change documents to determine that only approved specification changes were implemented.

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

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

f) Protect latest version of the source codes and databases.

4.2.6. Systems Documentation

The FI(s) shall:

a) Formulate procedures on systems 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 and 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.

4.2.7. Post-Implementation Review

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 BP&RD Circular No 9 dated 13th July, 2007 as amended from time to time.

4.4. Use of Cloud Services

a) Cloud computing is a service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage and services). Users of such services may not know the exact locations of servers, applications and data within the service provider's computing infrastructure for the hosting, storing or processing of information.
b) FI(s) shall perform enhanced level of due diligence for all forms of outsourcing arrangements involving cloud environment. Specifically, the FI(s) shall be aware of cloud computing unique attributes and risks especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality, regulatory compliance and auditing.
c) FI(s) shall segregate their data and applications into core and non-core categories to ensure that the core applications and business processes (*which use customer's identification and/or transactional data*) are not used in public cloud computing.
d) FI(s) shall ensure that applications/systems which use customer's identification (KYC/CDD) data and/or transactional data/information shall not be placed in a cloud environment.
e) The Cloud Service Provider (CSP) shall be located in Pakistan and all physical servers and services must be resided and operated from within Pakistan.
f) FI(s) shall ensure strict adherence to the following principles considering them as best practices while entering into an arrangement involving cloud computing:
   i) ***System & Location Transparency:*** Complete Transparency as to where data will be physically processed and stored.
   ii) ***Data Separation/Isolation:*** Customers' data must be segregated from other data held by the Service Provider.
   iii) ***Limits on Data Use:*** Customers' data will not be used for any other purpose other than that which is necessary to provide.
   iv) ***Security and Confidentiality:*** Customers should only contract for services with a Service Provider that has been certified to have to maintain robust security measures.

v) ***Audit & Access Rights:*** A Service Provider should provide access and inspection rights to regulators and to demonstrate compliance with all legal and contractual requirements.

vi) ***Review, Monitoring and Control:*** A Service Provider must demonstrate their compliance with agreed standards.

g) For all outsourcing arrangements with CSPs, FI(s) shall submit application for approval to SBP before entering into agreement with domestic CSP along with following documents:-

i) Risk Assessment Matrix

ii) Agreement with CSP

iii) Ownership structure of CSP

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 bank-wide process that defines how a bank is to respond to and recover from business disruptions in case of a disaster, enabling a bank to continue to support constituents and stakeholders alike.

5.1. Business Continuity Planning and Disaster Recovery Framework

The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capabilities of an FI. The FI(s) shall develop a comprehensive business continuity plan (BCP) as part of the business continuity planning process. The BCP shall be based on the size and complexity of the institution and should be consistent with the financial institution's overall business strategy. The goal of the BCP shall be to minimize financial losses to the institution, serve customers and financial markets with minimal disruptions, and mitigate the negative effects of disruptions on business operations. 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. The FI(s) shall maintain standby hardware, software and network components that are necessary for fast recovery. The FI(s) shall adopt a cyclical, process-oriented approach to business continuity planning. The BCP process, among other, may include:

a) Business Impact Analysis
b) Risk assessment
c) Disaster Recovery Plan
d) Disaster Recovery Testing

5.1.1 Business Impact Analysis

A business impact analysis (BIA) is the first step in the business continuity planning process and should include the:

a) Assessment and prioritization of all business functions and processes, including their interdependencies, as part of a work flow analysis;

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

c) Identification of the legal and regulatory requirements for the institution's business functions and processes;

d) Estimation of maximum allowable downtime, as well as the acceptable level of losses, associated with the institution's business functions and processes; and

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

5.1.2 Risk Assessment

The risk assessment is the second step in the business continuity planning process. Among others, it shall include:

a) Evaluating the BIA assumptions using various threat scenarios;

b) Analyzing threats based upon the impact to the institution, its customers, and the financial market it serves;

c) Prioritizing potential business disruptions based upon their severity, which is determined by their impact on operations and the probability of occurrence; and

d) Performing a "gap analysis" that compares the existing BCP to the policies and procedures that should be implemented based on prioritized disruptions identified and their resulting impact on the institution.

5.1.3. Disaster Recovery Plan

The FI(s) shall:

a) Include a scenario analysis to 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 (preferably not in the same metropolitan area) 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 of critical systems), with strategies such as engagement of different network service providers and alternate network paths.

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

5.1.4. Disaster Recovery Testing

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 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 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) During the tests especially DR testing, FI(s) should involve their Internal Auditors (including IS Auditors) and respective business group heads/ unit heads while signing-off test results of DR-BCP drills.

5.2 Data Backup Management

The FI(s) shall:

a) Develop and implement standard operating procedures for Data Management covering Data Storage, Retrieval, retention, Backup and disclosure of information in compliance with the legal framework that commensurate with the business requirements.

b) Carry out periodic testing and validation of the recovery capability of backup media and assess if the backup media is adequate and effective to support the recovery processes.

c) Encrypt and label backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.
d) Offsite storage area shall be adequately saved and well protected under authorized personnel.
e) Train key personnel on both the backup and restoration processes.

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 IT make the IT audit coverage essential to an effective overall audit program. The audit program should address IT risks throughout the organization, including the areas of IT management, strategic planning, IT operations, client/server architecture, local and wide-area networks, telecommunications, physical and information security, electronic products and services, systems development and acquisition and business continuity planning.

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 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 which shall be based on a 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) IT audit staff shall identify weaknesses, provide meaningful recommendations and review management's plans for addressing those weaknesses.

b) The audit function shall review 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) The audit function shall carry out 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.

d) The audit function may perform technical/specialized reviews such as conduct of periodic internal vulnerability assessment, penetration testing, incidents reports, computer forensics and review of emerging technologies, e.g., cloud computing, virtualization, mobile computing etc.

6.3 Reporting Methodology

The audit function shall:

a) Report the findings, conclusions and 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) Submit the report to the Audit Committee on periodical basis.

6.4 Post-closing/Monitoring Activities

a) The audit function shall ensure that senior management approve 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.