Guideline on ICT Security

Version 4.0, 2023

Bangladesh Bank

Preface

The technology landscape of the financial sector is changing at a rapid pace and the underlying information technology (IT) infrastructure supporting financial services grown in size and complexity in recent years. Digital transformation in the financial sector can be characterized by the introduction of new technologies and the use of existing ones in innovative ways to achieve greater automation and enrich financial service delivery.

While digital transformation offers significant benefits to the financial ecosystem, it also increases the exposure to a variety of technological risks, including cyber risks. The techniques used by cyber threat actors are becoming increasingly sophisticated, and weak links in the interconnected financial ecosystem can be compromised to conduct fraudulent financial transactions, exfiltrate sensitive financial data or disrupt the IT systems that support financial services. The increasing complexity of information and communication technology (ICT) and security risks, the increasing frequency of IT and security-related incidents as well as their potentially significant adverse impact on the operations of financial organizations. Moreover, due to the interconnectedness of the organizations, IT and security-related incidents risk causing systemic impacts. The introduction of emerging sustainable technology, formulation of proper security policies and practices, development of technology management skills and engagement of right human resources in the right place can overcome these challenges mostly.

Information security is essential to protect organizational assets against potential threats. Therefore, appropriate controls are required for an information security program with a broad, multi-layered security strategy**.**

This guideline set out how Bank and other Financial Organizations (FOs) should manage the IT and security risks that they are exposed to. In addition, this guideline is intended to provide the Bank/FO to which the guidelines apply a better understanding of supervisory expectations regarding the management of IT and security related risks.

Technical Committee

Chairman

Muhammad Zakir Hasan
Executive Director
Bangladesh Bank

Members

Khandaker Ali Kamran Al Zahid
Additional Director
Payment Systems Department
Bangladesh Bank

Mohammad Tauhidul Alam
Principle Maintenance Engineer
ICT Infrastructure Maintenance and Management Department
Bangladesh Bank

Fahad Zaman Chowdhury
Senior Maintenance Engineer & Member Secretary
ICT Infrastructure Maintenance and Management Department
Bangladesh Bank

Md. Kaderuzzaman
Joint Director (Ex-Cadre Law)
Law Department
Bangladesh Bank

Nurullah Shahin, Phd
Senior Maintenance Engineer
ICT Infrastructure Maintenance and Management Department
Bangladesh Bank

Md. Shafiqul Alam
Deputy Director
Banking Regulation and Policy Department
Bangladesh Bank

Md. Rakebul Islam Heru
Maintenance Engineer
ICT Infrastructure Maintenance and Management Department
Bangladesh Bank

Md. Masud Rana
Programmer/Asst.Systems Analyst
Information Systems Development and Support Department
Bangladesh Bank

Sohel Ahmed
Senior Information Security Officer
Cyber Security Unit (CSU)
Bangladesh Bank

Abdullah Al Maruf
Assistant Maintenance Engineer
ICT Infrastructure Maintenance and Management Department
Bangladesh Bank

Tuhin Talukder
Assistant Programmer
Information Systems Development and Support Department
Bangladesh Bank

Naima Akhter
Deputy General Manager
Sonali Bank Limited

Md. Mamunur Rashid
Deputy General Manager
Bangladesh Krishi Bank

Md. Mashuqur Rahman
EVP & Head of IT Division
The Premier Bank Limited

S. M. Mizanur Rahman
SVP & CISO
Islami Bank Bangladesh Limited

A B M Rezaul Hasan
Head Risk & Controls and Country Lead Information & Cyber Security
Standard Chartered Bank Limited

Rahat Azim
AGM & Head of Technology Infrastructure
IDLC Finance Limited

In addition, the following officials are also made contribution to prepare this guideline:

Sumit Kumar, Assistant Maintenance Engineer, Bangladesh Bank

Khandakar Rafiqual Islam, Head of Information Security, The City Bank Ltd.

Md. Faisal Hossain , AVP & Head of ICT Security Unit, Mercantile Bank Ltd.

Zahidur Rahman, AVP, Southeast Bank Ltd.

Table of Contents

[This page is left blank intentionally.]

Chapter 1: Introduction

The intricacy of information and communication technology (ICT) and consequent security risks are increasing in the financial sector at global scale. The frequency of ICT and security-related incidents (including cyber incidents) is rising, together with their potential significant adverse impact on financial organizations' operational activities. Moreover, due to the interconnectedness of financial organizations, ICT security-related incidents risk causing systemic impacts. Bangladesh Bank has responded to this by detailing how supervisor should cover ICT security risks within supervision, by detailing how financial organizations should manage outsourcing and by describing the expectations for ICT security management in this guideline. This guideline set out how banks and other financial organizations should manage the ICT and security risks that they are exposed to. In addition, this guidance aims to provide the banks and other financial institutions to which the guidelines apply with a better understanding of supervisory expectations for the management of ICT and security risks.

Information assets are critical to the services provided by the Banks and other financial organizations to their customers. ICT risk is also associated with a banking system that needs to be managed with thoughts and efforts. This revised version of the Guideline on ICT Security is to be used as a minimum requirement and as appropriate to the level of technology adoption of their operations.

1.1 Objectives

1.1 This Guideline defines minimum control requirements to which each the organization must adhere. The primary objectives of the Guideline are to:

a) Establish ICT Governance in the Financial Sector;
b) Help Organization developing their own ICT Security Policy;
c) Establish standard ICT Security Management approach;
d) Help Organization developing secure & reliable ICT infrastructure;
e) Establish secure environment for the processing of data;
f) Establish a holistic approach to ICT Risk management;
g) Establish a procedure for Business Impact Analysis in conjunction with ICT Risk Management;
h) Develop awareness of stakeholders' roles and responsibilities for the protection of information;
i) Prioritize information and ICT systems and associated risks those need to be mitigated;
j) Establish appropriate project management approach for ICT projects;
k) Ensure best practices (industry standard) of the usage of technology;
l) Develop a framework for timely and effective handling of operation and information security incidents;

m) Mitigate any interruption to business activities and protect critical business processes from the effects of major failures of information systems or disasters and ensure timely resumptions;
n) Define all the necessary controls required to protect data transmitted over communication networks;
o) Ensure that security is integrated throughout the lifecycle of information system acquisitions, development and maintenance;
p) Minimize security risks for electronic banking infrastructure including ATM and POS devices, payment cards, internet banking, mobile financial services, etc;
q) Build awareness and train the users associated with ICT activities for achieving the business objectives;
r) Harbor safe & secure usage of emerging technologies.

1.2 Applicability of the Guideline

a) The guideline is applicable to Bank, Non-bank Financial Institute (NBFI), Mobile Financial Service Provider (MFSP), Payment Service Provider (PSP), Payment System Operator (PSO) and other financial service provider regulated by Bangladesh Bank. Throughout this guideline all these institutions will be termed together as "**The Organization**".
b) All activities and operations require to ensure overall security including facility design, physical security, application security, network security, ICT risk management, project management, infrastructure security management, service delivery management, disaster recovery and business continuity management, alternative delivery channels management, acquisition and development of information systems, usage of hardware and software, disposal policy, protection of copyrights and other intellectual property rights, cloud security management, secure incident handling, identity & access management, cyber security management and emerging technology management.

1.3 Non-Compliance of the Guideline

1.3.1 The Organization shall assign a Team/Committee/Entity to monitor the compliance of the ICT security guidelines. A Team/Committee/Entity shall provide the initial observation of any non-compliance issue.
1.3.2 The Organization shall take initiatives to rectify the non-compliance activities as per ICT security guidelines within a specific time frame.
1.3.3 If The Organization fails to rectify the non-compliance activities within the time frame, penalty may be imposed depending on the impact of business or any adverse impact on customers' interest.

Chapter 2: ICT Governance

ICT Security Governance must ensure that the ICT functions and operations are efficiently and effectively managed. The top management needs to ensure that appropriate IT security controls are in place. They have to contribute to ICT security planning to ensure that resources i.e. process and technology is allocated consistently with business objectives and to ensure that sufficient and qualified technical staffs are employed. ICT Security Management is responsible for the ICT Governance of the Organization that includes but not limited to Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance and Risk coverage fund.

2.1 Roles and Responsibilities

The roles and responsibilities of the Board and Senior Management are crucial while implementing ICT Governance. ICT Governance stakeholders include the Board, ICT Steering Committee, ICT Security Committee, CEO/Managing Director, CIO, CTO, CITO, CISO, Risk Management Committee, Chief Risk Officer and Business Executives.

2.1.1 Roles and responsibilities of the Board are (but not limited to) as follows:

a) Approving ICT strategy and policies;
b) Ensuring that the management has placed an effective planning process;
c) Endorsing that the ICT strategy is indeed aligned with the business strategy;
d) Ensuring that the ICT organizational structure complements the business model and its direction;
e) Ensuring ICT investments represent a balance of risks and benefits with acceptable budgets;
f) Ensure Accountability;
g) Ensure compliance status of ICT Security Policy.

2.1.2 Roles and responsibilities of the ICT Steering Committee are (but not limited to) as follows:

ICT Steering Committee needs to be formed with representatives from ICT, Risk, HR, Cyber Security Unit, ICC/Audit, Legal and other related Business units.

a) Monitor the progress of achieving IT related strategic goals;
b) Aware of exposure towards ICT risks and controls;
c) Provide guidance related to risk, funding, or sourcing;
d) Ensure project priorities and assess feasibility for ICT proposals;
e) Consult and advise on the selection of technology maintaining standards;
f) Ensure compliance with regulatory and statutory requirements;
g) Ensure ICT architecture reflects the need for legislative and regulatory compliance.

2.1.3 Roles and responsibilities of the ICT Security Committee are (but not limited to) as follows:

ICT Security Committee needs to be formed with representatives from ICT, ICT/Cyber Security, Risk, ICC and Business units.

a) Ensure development and implementation of ICT security objectives, ICT security and risk related policies and procedures;
b) Provide ongoing management support to the Information Security processes;
c) Ensure continued compliance with the business objectives, regulatory and legal requirements related to ICT security;
d) Support to formulate an ICT risk management framework/process and establish acceptable ICT risk thresholds/ICT risk appetite and assurance requirements;
e) Periodic review and provide approval for modification in ICT Security processes.

2.2 ICT Policy, Standard and Procedure

2.2.1 The Organization must have an 'ICT Security Policy' that comply with this ICT Security Guideline and be approved by the Board. The policy shall have to be in line with this guideline.

2.2.2 The policy shall be reviewed annually at least.

2.2.3 The Organization shall engage ICT security professionals employed in separate ICT security departments/divisions/units/cells for improved and impartial dealing with security incidents, policy documentation, inherent ICT risks, risk treatments and other relevant activities.

2.2.4 For non-compliance issues, compliance plans shall be submitted to Bangladesh Bank. If any non-compliance issue persists due to exceptional case then dispensation can be taken from Bangladesh Bank. However, Dispensation shall be for a specific period.

2.2.5 The Organization shall maintain detailed design documents for all ICT critical infrastructures/ systems/services (e.g. Data Center design, Network design, Power Layout for Data Center etc.).

2.2.6 The Organization shall maintain an updated "Operating Procedure" for all ICT functional activities (e.g. Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery etc.).

2.2.7 The Organization shall have approved relevant requisition/acknowledgement forms for different ICT requests/operations/services.

2.2.8 The Organization shall have User Manual of all applications for internal/external users.

2.3 Organizational Structure and Documentation

2.3.1 The Organization shall have an approved and updated Organogram for the ICT departments/divisions.

2.3.2 The Organization shall have ICT support units/sections/personnel (Business/ICT) in the branch organogram.

2.3.3 ICT departments/divisions/units/sections shall have an approved Job Description (JD) for each staff with fall back.

2.3.4 The Organization shall maintain segregation of duties for ICT tasks.

2.3.5 The Organization shall have prescheduled roster for sensitive ICT tasks (e.g. EOD operation, Network Monitoring, Security Guard for Data Center, ATM Monitoring etc.).

2.3.6 The Organization shall analyze to ensure rational distribution of workload to their staffs.

2.4 Internal Information System Audit

2.4.1 Internal Information System (IS) audit shall be carried out by the Internal Audit/Compliance Department of the organization.

2.4.2 Internal IS audit shall be conducted by personnel with sufficient IS Audit experience, skills and professional certification.

2.4.3 The Organization shall use Computer-Assisted-Auditing Tools (CAATs) or similar automated tool to perform IS audit planning, monitoring/auditing, control assessment, data extraction/analysis, fraud detection/prevention and management.

2.4.4 An annual Information System audit plan shall be developed covering critical/major technology-based services/processes and ICT infrastructure including operational branches.

2.4.5 Internal Information System audit shall be done periodically at least once a year. The audit shall follow risk based approach based on criticality of the services. The report must be preserved for regulators as and when required.

2.4.6 The Organization shall ensure that audit issues are properly tracked and completely recorded, adequately followed up and satisfactorily rectified.

2.4.7 The Organization shall take appropriate measures to address the recommendations made in the last Audit Report.

2.5 External Information System Audit

2.5.1 The Organization shall engage qualified external auditor(s) for their information systems auditing in-line with their regular audit. The external audit shall be carried out at least annually.

2.5.2 The External Auditor shall have sufficient IS audit experience and professional certification for conducting audit activities.

2.5.3 The audit report shall be preserved for regulators as and when required. The

Organization shall take appropriate measures to address the recommendations made in the last Audit Report.

2.6 Standard Certification

2.6.1 The Organization may obtain industry-standard certification on area such as Information System Security, ICT Risk Management, Data Center Standard, Quality Management Systems, Software life cycle processes, Software Testing, Quality of ICT Service Delivery, Business Continuity Management, Payment Card Data Security etc.

2.7 Insurance or Risk Coverage Fund

2.7.1 Adequate insurance coverage or risk coverage fund shall be maintained so that costs of loss and/or damage of the ICT assets can be mitigated.

2.7.2 The risk coverage fund shall be maintained properly in the accounting system of the Organization, if applicable.

2.7.3 There shall have a clear policy to use risk coverage fund as a necessity if it is maintained.

Chapter 3: ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. The risks usually organization faces include strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, etc. In many enterprises, ICT-related risk is considered to be a component of operational risk. However, even strategic risk can have an ICT component itself, especially where ICT is the key enabler of new business initiatives. The same applies to credit risk, where poor ICT security can lead to lower credit ratings. It is better not to depict ICT risk with a hierarchic dependency on one of the other risk categories.

ICT risk is a business risk - specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within the organization. It consists of ICT-related events and conditions that could potentially impact the business.

3.1 ICT Risk Governance

3.1.1 ICT Risk Management Principle, Policy & Framework

3.1.1.1 The Organization shall begin Risk-aware Culture from the top with the Board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviours.

3.1.1.2 The Organization shall contribute to executive management's understanding of the actual exposure to ICT risk by open communication, enabling the definition of appropriate and informed risk responses.

3.1.1.3 The Organization shall confirm that proper Supply Chain Risk Management (SCRM) has been ensured.

3.1.1.4 The Organization shall establish a risk management framework to manage technology risks with appropriate processes, well-defined roles, responsibilities and clear reporting lines. The framework shall comprise the following essential components:

a) Risk Identification – identify assets, threats and vulnerabilities;

b) Risk Assessment – assess the potential impact and likelihood of threats;

c) Risk Treatment – implement processes and controls to manage risks;

d) Risk Monitoring and Review – monitor and review risks to remain aware of the current status;

e) Risk Reporting –report the risks as per the defined reporting line.

3.1.1.5 The Organization shall ensure that the ICT Risk Management Framework is documented and continuously improved, based on 'lessons learned' during its implementation and monitoring. The ICT and security risk management

framework shall be approved and reviewed, at least once a year.

3.1.2 Risk Management Committee

3.1.2.1 The Organization shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.

3.1.2.2 ICT security department/division/unit/cell shall report status of identified ICT security risk to the ICT Security Committee and Risk Management Committee periodically as defined in the policy.

3.1.2.3 The Organization shall define ICT risk management roles, responsibilities, and authorities of committees and individuals to contribute to the effectiveness of the ICT risk management system.

3.1.3 Risk Statement

3.1.3.1 The Organization shall define the Risk Appetite (amount of risk the organization is prepared to accept to achieve its' objectives) in terms of combinations of frequency and magnitude of a risk to absorb loss e.g., financial loss, reputation damage.

3.1.3.2 The Organization shall define the Risk Tolerance (tolerable deviation from the level set by the risk appetite definition) having approval from the board/Risk Management Committee and clearly communicated to all stakeholders.

3.1.3.3 The Organization shall develop and roll out the ICT risk Tolerance matrix to access the impact & likelihood of ICT risks against the given limit of ICT risk appetite set by the management.

3.1.3.4 The Organization shall review and approve risk appetite and tolerance change over time; especially for new technology, new organizational structure, new business strategy and other factors require the enterprise to reassess its risk portfolio at a regular interval.

3.1.3.5 The Organization shall define Risk Factors those influence the frequency and/or business impact of risk scenarios.

3.1.3.6 The Organization shall develop a set of metrics to serve as risk indicators. Indicators for risks with high business impact are most likely to be Key Risk Indicators (KRIs).

3.1.3.7 Selection of the right set of KRIs, The Organization shall carry out:

a) Provide an early warning for a high risk to take proactive action;

b) Provide a backward-looking view on risk events that have occurred;

c) Assist in continually optimizing the risk governance and management environment.

3.2 ICT Risk Assessment

Meaningful ICT risk assessments and risk-based decisions require ICT risks to be expressed in unambiguous and clear, business-relevant terms. Effective risk management requires mutual understanding between ICT and the business over which risk needs to be managed. All stakeholders must have the ability to understand and express how adverse events may affect business objectives.

3.1 ICT person shall understand how ICT-related failures or events can impact enterprise objectives and cause direct or indirect loss to the enterprise;

3.2 Business person shall understand how ICT-related failures or events can affect key services and processes.

3.2.1 Risk Identification

3.2.1.1 The Organization shall define the risk identification to determine the cause a potential loss and to gain insight into how, where and why the loss might happen.

3.2.1.2 The Organization shall identify asset owner, custodian and user for each asset, to provide responsibility and accountability for the asset. The asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment.

3.2.1.3 The threats should be identified generically and by type (e.g. unauthorized actions, physical damage, technical failures) and then where appropriate individual threats within the generic class identified.

3.2.1.4 The vulnerabilities should be identified to implement the effective controls on assets. Risk analysis should be considered depending on the criticality of assets, extent of vulnerabilities known and prior incidents involving in the organization.

3.2.2 Risk Analysis

3.2.2.1 The Organization shall perform risk analysis that can be based on qualitative risk analysis or quantitative risk analysis or combination of both that are described the scale of qualifying attributes to define magnitude of potential consequences (e.g. Low, Medium and High) or the scale with numerical values and likelihood, respectively.

3.2.2.2 The Organization shall roll out a Risk Assessment (RA) matrix based on the ICT risk tolerance matrix to identify the impact and likelihood of a risk to understand overall risk exposure of the institution.

3.2.2.3 ICT security department/unit/cell shall conduct periodic ICT risk assessment including inherent risks, residual risks of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.

3.2.2.4 The Organization shall establish business impact analysis needs to understand the effects of adverse events. The Organization may practice several techniques and options that can help them to describe ICT risks in business terms.

3.2.2.5 The Organization shall practice the development and use of *Risk Scenarios* technique to identify the important and relevant risks amongst all. The developed risk scenarios can be used during risk analysis where frequency and impact of the scenario are assessed.

3.2.3 Risk Evaluation

3.2.3.1 In conjuncture with the RA, The Organization shall also take measures to develop ICT risk treatment plans to establish necessary compensative controls, in order to reduce the identified risk & allow the organization to operate with the ICT risk appetite of the organization identified through the risk assessment matrix.

3.2.3.2 The Organization shall perform risk evaluation criteria to compare level of risks against risk evaluation criteria and risk tolerance criteria.

3.2.4 Control Design Assessment

3.2.4.1 The existing or planned controls should be identified to avoid unnecessary work or cost, e.g. in the duplication of controls and to ensure that the controls are working correctly.

3.2.4.2 The Organization shall assess whether the design of the actual control is sufficient to mitigate risks.

3.3 Risk Treatment & Control Monitoring

3.3.1 The Organization shall define the risk responsibilities to individuals and/or group for ensuring successful risk mitigation.

3.3.2 The Organization shall define the risk accountability applies to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset.

3.3.3 The Organization shall define risk response to bring risk in line with the defined risk appetite for the organization after risk analysis.

3.3.4 Risk treatment plans shall be reviewed and approved by ICT Risk Management committee.

3.3.5 The Organization shall record if any residual risks exist after implementation of approved treatment plan.

3.4 Risk Reporting & Escalation

3.4.1 The Organization shall implement risk reporting to reflect the overall health status of ICT and Security Risk based on the periodic risk treatment & control measurement outcome.

3.4.2 The Organization shall have formal risk escalation process which must identify who has the authority to accept the risk. Different types of risks such as strategic risk and operational risk may have different risk escalation matrix.

3.4.3 The Organization shall establish a central repository to record all such ICT risk events that caused significant impact on the business or franchise of the organization.

3.5 Risk Communication and Consultation

3.5.1 The Organization shall involve communicating the identified ICT risk between the responsible division/department and the concern stakeholders. The communication of ICT risk includes providing assurance of the outcome of the ICT risk management, share the results of the ICT risk assessment, support decision-making, improve awareness etc.

3.5.2 The Organization may engage the different stakeholders by conducting training, workshops, SWOT analysis, interviews, individual and group discussions, focus groups etc.

3.6 Risk Review and Monitoring

The Organization shall ensure that the following are continually monitored but not limited to:

a) New assets, threats, new or increased vulnerabilities that have been included in the ICT risk management scope;
b) Necessary modification of asset values;
c) ICT security incidents;
d) Configuration, Change Management etc.

Chapter 4: ICT Service Delivery Management

ICT Service Management covers the dynamics of technology operation management that includes capacity management, request management, change management, incident and problem management etc. The objective is to set controls to achieve the highest level of ICT service quality by minimum operational risk.

4.1 Service Request Management

4.1.1 All requests for ICT services must be approved by an authorized entity defined by the Organization.

4.1.2 The Organization shall maintain a service catalog with complete list of services. The service catalog must be kept up to date.

4.1.3 The Organization may have an internal web portal where all users can go to initiate service requests.

4.1.4 There shall be approved workflow for common service request types which describes the approval process, service delivery process responsibility and other aspects of the service.

4.2 Change Management

4.2.1 Changes to information processing facilities and systems shall be controlled.

4.2.2 The Organization shall maintain all the standard documentation of change management such as Business Requirement Document (BRD) which will cover the requirements of system changes and the impact that will have on business processes, security matrix, reporting, interfaces etc.

4.2.3 All changes of business application implemented in the production environment must be governed by a formal documented process with necessary change details.

4.2.4 Audit trails shall be maintained for business applications.

4.2.5 The Organization shall prepare rollback plan for unexpected situation.

4.2.6 User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment.

4.2.7 User Verification Test (UVT) for post deployment may be carried out.

4.3 Incident Management

An incident occurs when there is an unexpected disruption to the standard delivery of ICT services. The Organization shall appropriately manage such incidents to avoid a situation of mishandling that results in a prolonged disruption of ICT services.

4.3.1 The Organization shall establish an incident management framework with the

objective of restoring normal ICT service as quickly as possible following the incident with minimal impact to the business operations. The Organization shall also establish roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating and monitoring incidents.

4.3.2 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, the organization may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. The Organization shall train helpdesk staff to determine incidents of high severity level. In addition, criteria used for assessing severity levels of incidents shall be established and documented.

4.3.3 The Organization shall establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident.

4.3.4 The predetermined escalation and response plan for security incidents shall be tested on a periodic basis.

4.3.5 The Organization shall form an ICT Emergency Response Team, comprising staff within the organization with necessary technical and operational skills to handle major incidents.

4.3.6 In some situations, major incidents may further develop adversely into a crisis. Senior management shall be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis. The Organization shall inform Bangladesh Bank as soon as possible in the event of a critical system has failed over to its disaster recovery system.

4.3.7 The Organization shall keep customers informed of any major incident. Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the organization.

4.3.8 The Organization shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

4.4 Problem Management

While the objective of incident management is to restore the ICT service as soon as possible, the aim of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated incidents.

4.4.1 The Organization shall establish a process to log the information system related problems.

4.4.2 The Organization shall have the process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.

4.4.3 Problem findings and action steps taken during the problem resolution process

shall be documented.

4.4.4 As incidents may trail from numerous factors, the organization shall perform a root cause and impact analysis for major incidents which result in severe disruption of ICT services. The Organization shall take remediation actions to prevent the recurrence of similar incidents.

4.4.5 The root-cause and impact analysis report shall cover following areas:

a) Root Cause Analysis
   i. When did it happen?
   ii. Where did it happen?
   iii. Why and how did the incident happen?
   iv. How often had a similar incident occurred over last 2 years?
   v. Did detection occur promptly?
   vi. What lessons were learnt from this incident?

b) Impact Analysis
   i. Extent of the incident including information on the systems, resources, customers that were affected;
   ii. Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence;
   iii. Breach of regulatory requirements and conditions as a result of the incident.

c) Corrective and Preventive Measures
   i. Immediate corrective action to be taken to address consequences of the incident. Priority shall be placed on addressing customers' concerns.
   ii. Measures to address the root cause of the incident.
   iii. Measures to prevent similar or related incidents from occurring.

4.4.6 A trend analysis of past problems shall be performed to facilitate the identification and prevention of similar problems.

4.5 Capacity Management

The goal of capacity management is to ensure that ICT capacity meets current and future business requirements in a cost-effective manner.

4.5.1 To ensure that ICT systems and infrastructure are able to support business functions, the organization shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.

4.5.2 The Organization shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and business requirements effectively.

4.5.3 The Organization shall prevent resources from being unavailable by implementing

fault tolerance mechanisms, prioritizing tasks and equitable resource allocation mechanisms.

4.5.4 The Organization shall ensure the timely acquisition of required capacity, taking into account aspects such as resilience, contingency, workloads and storage plans.

4.5.5 The Organization may use modeling tools to assist with the prediction of capacity, configuration reliability, performance and availability requirements.

4.6 Migration Management

4.6.1 The Organization shall have a Migration Policy indicating the requirement of roadmap/ migration plan / methodology for data migration.

4.6.2 The Organization shall ensure the data confidentiality, integrity, completeness and consistency of data during the migration process as follows:

a) Data shall be backed up before migration for future reference or any emergency that might arise out of the data migration process.
b) Data shall not be altered manually or electronically by a person, programmer, substitution or overwriting in the new system.
c) The total number of records from the source database is transferred to the new database.
d) New application shall be consistent/ compatible with that of the original application.

4.6.3 The Organization shall maintain the last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform separately in the archive for any future reference.

4.6.4 The error logs pertaining to the pre-migration/ migration/ post migration period along with root cause analysis and action taken need to be available for review.

Chapter 5: Infrastructure Security Management

The ICT landscape is vulnerable to various forms of attacks. The frequency and malignancy of such attacks are increasing. It is imperative that the organization implements security solutions at the data, application, database, operating systems and networks to adequately address related threats. Appropriate measures shall be implemented to protect sensitive or confidential information such as customer personal information, account and transaction data which are stored and processed in systems. Customers shall be properly authenticated before access to online transactions, sensitive personal or account information.

5.1 Asset Management

5.1.1 Asset Acquisition Management

5.1.1.1 Prior to procuring any new ICT assets, compatibility, feasibility, applicability, availability assessment (with existing system) shall be performed by the organization.

5.1.1.2 All ICT asset procurement shall be complied with the procurement policy of the organization.

5.1.1.3 Each ICT asset shall be assigned to a custodian (an individual or entity) who will be responsible for the development, maintenance, usage, security and integrity of that asset.

5.1.2 Inventory Management

5.1.2.1 All ICT assets shall be clearly identified and labeled. Labeling shall reflect the established classification of assets.

5.1.2.2 The Organization shall identify all important information assets along with fixed assets and draw up and maintain an ICT asset inventory stating significant details (e.g. owner, custodian, purchase date, location, license number, configuration, End of Support, End of Life etc.).

5.1.2.3 The Organization shall review and update the ICT asset inventory periodically.

5.1.2.4 ICT asset inventory shall be adequately protected (preferably using automated ICT asset or inventory management solution) from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

5.1.3 License Management

5.1.3.1 The Organization shall comply with the terms of all software licenses and shall not use any software that has not been legally purchased or otherwise legitimately obtained.

5.1.3.2 Outsourced software used in production environment shall be subjected to support agreement with the vendor.

5.1.3.3 The Organization shall approve list of Software which will only be used in any computer.

5.1.3.4 Use of unauthorized or pirated software must strictly be prohibited throughout the organization.

5.1.3.5 The Organization shall take appropriate measures to find out non-compliance / under-licensed software.

5.1.4 Asset Transfer and Distribution

5.1.4.1 The Organization shall formulate guidelines for the use of portable devices, especially for the usage at outside premises.

5.1.4.2 The Organization shall define a policy regarding organizational assets return back from employees/external parties upon termination of their employment, contract or agreement.

5.1.5 Asset Disposal

5.1.5.1 The Organization shall establish a Disposal Policy for information system asset protection. All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or re-issue.

5.2 Data Center Management

5.2.1 Data Center Classification

5.2.1.1 The Organization shall establish and classify/assess their data center/DR Site as one of the following categories. Recommended category Tier 1/Rated1 to Tier 4/ Rated 4 based on their business requirements.

5.2.1.2 The Organization with Tier 1/ Rated 1 data center shall meet the following criteria:

a) No more than 28.8 hours of downtime per annum;
b) 99.671 % uptime per annum;
c) No redundancy.

5.2.1.3 The Organization with Tier 2/ Rated 2 data center shall meet the following criteria:

a) No more than 22 hours of downtime per annum;
b) 99.741 % uptime per annum;
c) Partial cooling and multiple power redundancies.

5.2.1.4 The Organization with Tier 3 / Rated 3 data center shall meet the following criteria:

a) N+1 (the amount required for operation plus a backup) fault tolerance;
b) 72 hours of protection from power outages;
c) No more than 1.6 hours of downtime per annum;
d) 99.982 % uptime per annum.

5.2.1.5 The Organization with Tier 4/ Rated 4 data center shall meet the following

criteria:

a) Zero single points of failure;
b) 99.995 % uptime per annum;
c) 2N+1 infrastructure (two times the amount required for operation plus a backup);
d) No more than 26.3 minutes of downtime per annum as a maximum figure;
e) 96-hour power outage protection.

5.2.1.6 Based on the criticality of applications and data, the organization shall determine the best suited Disaster recovery site for their respective operations. They can select - Hot site, Warm site, and Cold site, based on their respective requirements.

5.2.1.7 The Organization with Hot site shall meet the following criteria:

a) Hot site is a backup site, which shall up and running continuously. It shall allow the organization to continue normal business operations, within a very short period of time after a disaster. Hot site shall be online and must be available immediately;
b) Hot site shall be equipped with all the necessary hardware, software, network, and Internet connectivity;
c) Data shall regularly back up or replicated to the hot site so that it can be made fully operational in a minimal amount of time in the event of a disaster at the original site;
d) Hot site shall be located far away from the original site, in order to prevent the disaster affecting the hot site also;
e) Hot site shall be used for business-critical apps;
f) Hot site may be of two type-
   i) Active-Active = Both sides are alive;
   ii) Active-Passive = Data is replicated in passive site.

5.2.1.8 The Organization with Warm site shall meet the following criteria:

a) Warm site is another backup site, which is not as equipped as a Hot site. Warm Site shall configure with power, phone, network etc;
b) Warm site may have servers and other resources;
c) In Warm site data is replicated but servers may not be ready.

5.2.1.9 The Organization with Cold site shall meet the following criteria:

a) Cold site contains even fewer facilities than a Warm site;
b) Space and associated infrastructure (e.g., power, telecoms and environmental controls to support IT systems) shall only be installed when disaster recovery (DR) services are activated.

5.2.1.10 The Organization shall take permission from Bangladesh Bank prior to establish of new DC/DR or migration of their existing DC or DR to different location or different entity.

5.2.2 Physical Security (Including Rack, CCTV)

5.2.2.1 The following factors need to be considered before selecting the location of Data Center: geological activity like earthquakes, high-risk industries in the area, risk of flooding and risk of force majeure (war, riots, fire, flood, hurricane, typhoon, earthquake, lightning, explosion, strikes, lockouts, slowdowns, prolonged shortage of energy supplies and acts of state or governmental action prohibiting etc.)

5.2.2.2 Physical security shall be applied to the information processing area or Data Center. DC must be a restricted area and unauthorized access shall be strictly prohibited.

5.2.2.3 The Data Center area shall be protected with intelligent video surveillance system along with video analytics to detect individuals, track objects, track movement, avoid false alarms and check for any illegal activity.

5.2.2.4 The Organization shall limit access to DC to authorized staff only. The Organization shall only grant access to the DC on a need to have basis. Physical access of staff to the DC shall be revoked immediately if it is no longer required.

5.2.2.5 Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. The Organization shall ensure that visitors are always accompanied by an authorized employee while in the DC.

5.2.2.6 Access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center.

5.2.2.7 All physical access to sensitive areas must be logged with purpose of access into the Data Center.

5.2.2.8 The Organization shall ensure that the perimeter of the DC, facility and equipment room are physically secured and monitored. The Organization shall employ physical, human and procedural controls for 24 hours such as the use of security guards, card access system, mantraps and surveillance system where appropriate.

5.2.2.9 Emergency exit door shall be available.

5.2.2.10 Data Center must have a designated custodian or manager in charge (an individual or entity) to provide authorization and to ensure compliance with policy.

5.2.2.11 An inventory of all computing equipment, associated equipment and consumables housed in DC must be maintained by the manager or a delegate.

5.2.2.12 Where DC is operated by an outsourced service supplier, the contract between the bank and supplier must indicate that all the requirements of policy regarding physical security must be complied with and that the organization reserves the right to review physical security status at any time.

5.2.2.13 Where DC is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to use for the organization must be reviewed and authorized by The Organization itself.

5.2.2.14 The physical security of Data Center premises shall be reviewed at least once

each year.

5.2.2.15 Server/network room/rack must have protected with lock and key under a responsible person for both front and back door**.**

5.2.2.16 Physical access shall be restricted, visitors log must exist and to be maintained for the server room.

5.2.2.17 Access authorization list must be maintained and reviewed on regular basis.

5.2.2.18 There shall be a provision to replace the server and network devices within shortest possible time in case of any disaster.

5.2.2.19 Server/network room/rack shall be provisioned with appropriate cooling system. Water leakage precautions and water drainage system from Air Conditioner shall be installed.

5.2.2.20 Rack in the Data Center must be protected to meet Earthquake Safety guidelines.

5.2.2.21 Power generator shall be in place to continue operations in case of power failure.

5.2.2.22 Fuel of power generator shall be kept sufficient to meet the demand in case of national blackout or other similar incidents.

5.2.2.23 UPS shall be in place to provide uninterrupted power supply to the server and required devices.

5.2.2.24 Immediate measure must be taken on overloading electrical outlets with too many devices.

5.2.2.25 Address and phone numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT/ responsible personnel) must be available to cope with any emergency situation.

5.2.3 Environmental Security

5.2.3.1 Protection of Data Center from the risk of damage due to fire, flood, explosion & other forms of disaster shall be designed and applied. To build Data Center and Disaster Recovery Site in multi-tenant facilitated building is discouraged.

5.2.3.2 Layout design of Data Center including power supply and network connectivity shall be properly documented.

5.2.3.3 Water detection devices shall be placed below the raised floor if it is raised.

5.2.3.4 Any accessories or devices not associated with Data Center and powered off devices shall not be allowed to store in the Data Center. Separate storeroom must be in place to keep all sorts of unused and redundant IT equipment's.

5.2.3.5 The sign of "No eating, drinking or smoking", "Emergency Exit" shall be in display.

5.2.3.6 Dedicated office vehicles for any of the emergencies shall always be available on-site. Availing of public transport must be avoided while carrying critical equipment's outside the bank's premises to avoid the risk of any causality.

5.2.3.7 Data Center shall have dedicated telephone communication.

5.2.3.8 Power supply system and other support units must be separated from production site and placed in secure area to reduce the risks from environmental threats.

5.2.3.9 Power supply from source (Main Distribution Board or Generator) to Data Center must be dedicated. Electrical outlets from these power sources for any other devices must be restricted and monitored to avoid the risk of overloading.

5.2.3.10 The following environmental controls shall be installed:

a) Uninterrupted Power Supply (UPS) with backup units;
b) Backup Power Supply;
c) Temperature and humidity measuring devices;
d) Water leakage precautions and water drainage system from Air Conditioner;
e) Cooling System with backup units. Industry standard cooling system shall be in place to avoid water leakage from the conventional air conditioning system;
f) Emergency power cut-off switches where applicable;
g) Emergency lighting arrangement;
h) Dehumidifier for humidity control.

5.2.3.11 The above-mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 basis.

5.2.4 Fire Prevention

5.2.4.1 The Organization shall carry out a Fire Risk Assessment**.**

5.2.4.2 The Organization shall use fire-resistant rated construction for the data center and IT equipment rooms. Wall, ceiling and door of Data Center shall be fire-resistant.

5.2.4.3 Auto Fire Detection & Suppression System (AFSS) shall be installed and tested periodically. It's important to have a fire alarm or other fire suppression system in case of emergency.

5.2.4.4 Early smoke detector system/ Aspiration Smoke Detection System shall be installed and tested periodically.

5.2.4.5 There shall be fire detector below the raised floor if it is raised.

5.2.4.6 The Organization shall ensure the necessary portable fire extinguisher provision. Everyone in the data center must know how to operate a fire extinguisher.

5.2.4.7 The Organization shall train all personnel working in the data center on what to do in a fire-related emergency.

5.2.4.8 Flammable items such as paper, wooden items, plastics etc. shall not be allowed to store in the data center and data center area.

5.2.4.9 The Organization shall ensure the data center room is well ventilated.

5.2.5 Cable Management

5.2.5.1 The Organization shall have a proper cabling management plan.

5.2.5.2 After planning the organization shall determine the entry path of the cables into the IT rack i.e., whether the cables will enter the IT rack through the roof or the floor. If entering from the top, the location of IT rack roof cutouts and their proximity to the vertical cable channels need to be considered. If entering from the

bottom (the cables will most likely run under a raised floor), eliminate any obstructions in the base that can interfere with the cable entry path.

5.2.5.3 After determining the cable entry path, the organization shall separate power and data cables to prevent erratic or error-prone data transfers. To minimize the effects of EMI, power cables shall be segregated from data cables as much as practical.

5.2.5.4 The Organization shall ensure that copper data cables and fiber optic cable runs are separated, because the weight of copper cables can damage the fiber.

5.2.5.5 The Organization shall maintain a consistent cable jacket color coding standard for each type of cable in the tray, copper, fiber, telecommunication, Power over Ethernet (PoE), and high voltage power lines for easy identification, expansion, and repairs.

5.2.5.6 The Organization shall label cables securely on each end.

5.2.5.7 The Organization shall secure cables and connectors to prevent excessive movement and to provide strain relief of critical points.

5.2.5.8 After cables are installed and labeled, the organization shall ensure that the airflow path is clear of obstructions.

5.2.5.9 After installing the cable, the organization shall document the complete infrastructure including diagrams, cable types, patching information, and cable counts and keep this information easily accessible to data center personnel and assign updates to one or more staff members and maintain organization.

5.2.6 Data Center Capacity Management

Data center capacity management establishes an organizational strategy for managing network and device resources, power load, cooling capacity and storage to ensure workload demands of users and customers.

5.2.6.1 The Organization shall conduct a comprehensive inventory of devices, hardware, and software which include all relevant dependencies and configurations that could impact the data center functions.

5.2.6.2 The Organization shall complete an inventory of upcoming projects, upgrades, or expansions to the network, business or project and client scopes.

5.2.6.3 The Organization shall agree on Performance Metrics i.e. what will be monitored, and what values are acceptable. The Organization need to determine the data center performance metric values they are comfortable with i.e. how long Organization store data for, what application response times should be, what uptime should be, and so on.

5.2.6.4 After establishment of data center inventory and baseline performance, the organization may check data center regularly for performance changes or issues and for rapid increases in capacity or malfunctioning devices. With historical gaps or a lack of current data, it can be difficult to accurately predict regular capacity changes.

5.2.6.5 The Organization shall use Data Center Capacity Planning Tools with capacity planning, performance and storage management capabilities which can automate

parts of the process, help to make things faster and more efficient, eliminate inaccuracies and cut down on the time IT staff spends troubleshooting and maintaining the data center.

5.3 Data Security Management

The Organization shall establish a data security management policy that is appropriate to the purpose of the organization and must include data security objectives or provides the framework for setting data security objectives. The policy shall be communicated within the Organization and be available to interested parties as appropriate.

5.3.1 Data Classification

5.3.1.1 The Organization shall have a well-defined process for data classification where it mentions how it classifies and labels data.

5.3.1.2 The Organization may classify information in terms of confidentiality:

a) Restricted (only senior management have access);
b) Confidential (most employees with designated roles have access);
c) Internal (all employees have access);
d) Public information (everyone has access).

5.3.1.3 The Organization may define less or more levels depending on their own requirement or complexity of data management.

5.3.2 Data Retention

5.3.2.1 The Organization shall develop a data retention policy based on legal, regulatory and business requirement.

5.3.2.2 Retention period for each data asset shall be clearly defined. Different data should have different retention periods.

5.3.2.3 The Organization shall delete the data that no longer serves a purpose to the Organization or has been held for the required retention period.

5.3.2.4 The Organization shall review the data retention policy on a regular basis.

5.3.3 Data Custodianship

Data Custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules. Simply put, Data Stewards are responsible for what is stored in a data field, while Data Custodians are responsible for the technical environment and database structure.

5.3.3.1 The Organization shall assign data custodian for each data asset.

5.3.3.2 Data Custodian shall maintain physical security, system security and safeguard appropriate to the classification level of the data in their custody.

5.3.3.3 Data Custodian will maintain disaster recovery plans and facilities appropriate to business needs.

5.3.4 Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration or unwanted destruction of sensitive data.

5.3.4.1 The Organization shall develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorized access, modification, copying, or transmission of its sensitive data keeping into consideration of all states of data – data in motion, data at rest and data in use.

5.3.4.2 The Organization shall implement appropriate measures to prevent and detect data theft, as well as unauthorized modification in systems and endpoint devices. The Organization shall ensure systems managed by the FI's service providers are accorded the same level of protection and subject to the same security standard.

5.3.4.3 Confidential data stored in systems and endpoint devices shall be encrypted and protected by strong access controls.

5.3.4.4 The Organization shall ensure only authorized data storage media, systems and endpoint devices are used to communicate, transfer or store confidential data.

5.3.4.5 The Organization shall implement security measures to prevent and detect the use of unauthorized internet services which allow users to communicate or store confidential data. For examples, services include social media, cloud storage and file sharing, web email and messaging applications.

5.3.4.6 The Organization shall ensure confidential data is deleted from storage media, systems and endpoint devices before they are redeployed or disposed of.

5.4 Server Security Management

5.4.1 Physical/Conventional Server Security

5.4.1.1 Users shall have specific authorization for accessing servers with defined set of privileges.

5.4.1.2 Additional authentication mechanism shall be used to control access of remote users.

5.4.1.3 Inactive session shall be expired after a defined period of inactivity.

5.4.1.4 Activities of System Administrators shall be logged. Servers containing sensitive and confidential data may export activity logs to a central log host.

5.4.1.5 The Organization shall maintain test server(s) to provide a platform for testing of configuration settings, new patches and service packs before applied on the production system.

5.4.1.6 The Organization shall ensure the security of file sharing process. File and print shares must be disabled if not required or kept at a minimum where possible.

5.4.1.7 All unnecessary services running in the production server shall be disabled. Any new services shall not run-in production server without prior testing.

5.4.1.8 All unnecessary programs shall be uninstalled from production servers.

5.4.2 Virtual Server Security

5.4.2.1 The Organization shall plan of setting limit on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM.

5.4.2.2 Host and guest Operating System (OS) must be updated with new/required security patches and other patches if necessary. Patching requirements shall also be applied to the virtualization software.

5.4.2.3 Like physical servers, virtual servers need to be backed up regularly.

5.4.2.4 The Organization shall ensure that host and guests use synchronized time**.**

5.4.2.5 File sharing shall not be allowed between host and guest OSs, if not required.

5.4.3 Server Hardening

5.4.3.1 The Organization shall remove/disable un-needed/un-used software and services.

5.4.3.2 The Organization shall remove unnecessary system accounts or disable guest account. .

5.4.3.3 The Organization shall make changes (rename, disable, change default password, etc.) to default accounts.

5.4.3.4 The Organization shall only enable required network ports.

5.4.3.5 The Organization shall install patches from a trusted source in a timely fashion.

5.4.3.6 The Organization shall update firmware from a trusted source.

5.4.3.7 The Organization shall install and maintain up-to-date malware protection.

5.4.3.8 The Organization shall ensure server-network access control.

5.5 Network Security Management

The Organization shall establish baseline standards to ensure security for Operating Systems, Databases, Network equipment and portable devices which shall meet organization's policy. They shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

5.5.1 Internet Access Management

5.5.1.1 Internet access shall be provided to employees according to the approved Internet Access Management Policy.

5.5.1.2 Access to and use of the internet from bank premises must be secure and must not compromise information security of the organization.

5.5.1.3 Access to the Internet from bank premises and systems must be routed through secure gateways.

5.5.1.4 Any local connection directly to the Internet from the organization premises or systems, including standalone PCs and laptops, is prohibited unless approved by

appropriate authority.

5.5.1.5 Employees shall be prohibited from establishing their own connection to the Internet using organizations' systems or premises.

5.5.1.6 Use of locally attached modems with banks' systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.

5.5.1.7 Internet access provided by the organization must not be used to transact any commercial business activity that is not done by the organization. Personal business interests of staff or other personnel must not be conducted.

5.5.1.8 Internet access provided by the organization must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.

5.5.1.9 All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.

5.5.1.10 The Organization shall install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical stages of its ICT infrastructure to protect the network perimeters.

5.5.2 Remote Access Management

Remote access solutions typically need to support several security objectives. These can be accomplished through a combination of security features built into the remote access solutions and additional security controls applied to the client devices and other components of the remote access solution.

To achieve these objectives, all the components of remote access solutions including client devices, remote access servers and internal servers accessed through remote access should be secured against a variety of threats.

5.5.2.1 The Organization shall develop a remote access security policy that defines remote access and BYOD requirements.

5.5.2.2 The Organization shall ensure that remote access servers are secured effectively and configured to enforce remote access security policies. The Organization also ensure that remote access servers are kept with up-to-date patches and that they can only be managed from trusted hosts by authorized administrators.

5.5.2.3 The Organization shall consider the network placement of remote access servers.

5.5.2.4 The Organization shall make risk-based decisions about what levels of remote access should be permitted from which types of client devices.

5.5.2.5 If external device use (e.g., BYOD, third-party controlled) is permitted within the organization's facilities, the organization shall strongly consider establishing a separate, external, dedicated network for this use with remote access policies. Allowing BYOD and third party controlled client devices to be directly connected

to internal enterprise networks adds risk as these devices do not have the same security safeguards as the organization's own devices.

5.6 Local Area Network/Wide Area Network Management

5.6.1 WAN Management

5.6.1.1 The Organization shall establish redundant communication links for WAN connectivity.

5.6.1.2 Unauthorized access and electronic tampering shall be controlled strictly. Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.

5.6.1.3 The Network Design and its security configurations shall be implemented under a documented plan. There shall have different security zones defined in the network design.

5.6.1.4 The Organization shall deploy firewalls or other similar measures within internal networks to minimize the impact of security exposures originating from third party or overseas systems as well as from the internal trusted network.

5.6.1.5 SYSLOG Server may be established depending on Network Size to monitor the logs generated by network devices.

5.6.1.6 Authentication Authorization and Accounting (AAA) Server shall be established depending on Network Size to manage the network devices effectively.

5.6.1.7 Role-based and/or Time-based Access Control Lists (ACLs) shall be implemented in the routers to control network traffic.

5.6.1.8 Real time health monitoring system for infrastructure management shall be implemented for surveillance of all network equipment and servers.

5.6.1.9 Connection of personal laptop to office network or any personal wireless modem with the office laptop/desktop must be restricted and secured.

5.6.1.10 The Organization shall change all default passwords of network devices.

5.6.1.11 All unused ports of access switch shall be shut-off by default if otherwise not defined.

5.6.1.12 All communication devices shall be uniquely identifiable with proper authentication.

5.6.2 LAN Management

5.6.2.1 Groups of information services, users and information systems shall be segregated in networks, e.g. VLAN.

5.6.2.2 The Organization shall use IP-MAC binding/ or other effective methods in their LAN so that unauthorized devices can't be connected.

5.6.2.3 The Organization shall ensure physical security of all network equipment.

5.6.2.4 The Organization shall use high quality devices to setup LAN for reliability.

5.6.2.5 The Organization shall segregate Guest Network with only required privileges.

5.6.2.6 Secure Login feature (i.e. SSH) shall be enabled in network devices for remote

administration purposes. Any unencrypted login option (i.e. TELNET) shall be disabled.

5.6.2.7 The Organization shall install network security devices, such as firewalls as well as intrusion detection and prevention systems at critical stages of its ICT infrastructure to protect the network perimeters.

5.6.2.8 The Organization shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant.

5.6.3 Wi-Fi Management

5.6.3.1 The Organization shall maintain/update an inventory of all Access Points (AP) and wireless devices.

5.6.3.2 The Organization shall segregate corporate network from the Wi-Fi network physically/logically with strong controls.

5.6.3.3 Default vendor configurations shall be changed on all wireless access points.

5.6.3.4 Default passwords/passphrases shall be changed on all wireless access points and strong administrative passwords should be utilized.

5.6.3.5 Any other security-related vendor default settings shall be changed, as applicable, on all wireless access points.

5.6.3.6 Server Set Identifier (SSID) shall be set to a unique identifier.

5.6.3.7 Strong encryption technology shall be utilized. If the wireless devices do not support strong encryption for authentication/transmission over wireless networks, the firmware on these devices should be upgraded or these devices should not be utilized within the wireless network.

5.6.3.8 Software security patches shall be tested and deployed on a regular basis.

5.6.3.9 If the reset function is ever utilized on a wireless access point, the access point shall be restored to the latest security settings.

5.6.3.10 Wireless access points should be placed in secure locations with restricted access.

5.6.3.11 The Organization shall review wireless audit logs on a regular basis and maintained securely on a log server.

5.6.3.12 The Organization shall search Rogue wireless access points routinely at least on a quarterly basis and any suspicious devices discovered should be promptly reported to the security team in accordance with the incident response plan, process and procedure.

5.6.3.13 All wireless clients shall have anti-virus installed, personal firewalls configured and all file sharing on wireless enabled devices should be disabled.

5.6.3.14 All personnel shall obtain authorization prior to utilizing the wireless access point and shall agree to the liability disclaimer prior to utilizing this resource.

5.7 Storage Security Management

5.7.1 The Organization shall restrict physical access to storage fabric.

5.7.2 The Organization shall restrict access to storage management network using firewall or Access Control List (ACL). Management ports such as serial port, console port shall be disabled when not in use.

5.7.3 LAN interface used for management traffic shall be segregated by physical isolation. Virtual LAN (VLAN) may be used where physical isolation is not possible.

5.7.4 The Organization shall properly secure supporting infrastructure to ensure security of the storage system.

5.7.5 The storage system shall be sufficiently hardened with standard security practices such as disabling unused services, prohibiting less secure protocols etc.

5.7.6 The Organization shall ensure that firmware, operating system and application are up-to-date and known vulnerabilities are remediated as quickly as possible.

5.8 Application Security Management

5.8.1 The Organization shall evaluate all new applications to determine their risk and suitability for installation in the production environment.

5.8.2 Applications that require authentication must be configured with password policy having appropriate complexity. The Organization may enhance security of the application by setting up multi-factor authentication where possible.

5.8.3 All changes to the existing application shall be made in compliance with Change Control Procedures.

5.8.4 The Organization shall ensure security patches are deployed on timely manner and known vulnerabilities are remediated as quickly as possible.

5.9 Database Security Management

5.9.1 User accounts & user rights shall be defined. Password and profile policies shall be set up, strong passwords policy shall be enforced and roles shall be used to limit user access to data.

5.9.2 Access Control systems shall include File permissions, Program permissions & Data rights.

5.9.3 All access to any database containing cardholder data (including access by applications, administrators, and all other users) shall be restricted.

5.9.4 Privilege review shall be conducted to identify privileges that are being used, track the source of the privileges and identify privileges that are not being used.

5.9.5 Access to cardholder database shall be driven through two factor authentication.

5.9.6 Database shall not be accessible through the Internet.

5.9.7 Database that stores cardholder data shall be placed in an internal network zone,

segregated from the DMZ and other untrusted networks.

5.9.8 Database audit trail need to be configured to log all audit trails and send to centralized log solution.

5.9.9 Role based Access to DB shall be implemented.

5.9.10 Database related hardware and software shall be hardened as per baseline security.

5.9.11 Cryptographic Services shall be used to protect and validate information at rest, in transit, and in use.

5.9.12 Database shall be restored in the test environment for testing backup quality and for practice in case of disaster in DC.

5.10 Endpoint Security Management

5.10.1 The Organization must ensure that any private, sensitive or confidential information that is stored on Endpoint device has the appropriate security controls to restrict and prevent retrieval or intercept by an unauthorized person or party.

5.10.2 Operating Systems (OS), endpoint software and application software are to be kept up to date with the latest security related patches.

5.10.3 OSs that reached end of support life shall not be permitted to connect to the organization network.

5.10.4 All endpoint devices connected to the Organization's internal network must be protected by end point security protection and must be running the latest virus definitions to accurately detect the latest viruses and malware.

5.10.5 Disabling or removing of end point protection or disabling of signature definition updates on endpoints is prohibited.

5.11 System Upgrade & Patch Management

5.11.1 The Organization shall establish and ensure that the patch management procedures include identification, categorization and prioritization of security patches. To implement security patches in a timely manner, the organization shall establish the implementation time frame for each category of security patches.

5.11.2 The Organization shall perform testing of security patches before deployment into the production.

5.11.3 The Organization shall document patch management procedure. The document must include scope, roles and responsibilities, timeline, functional guidelines, and procedures. The scope should outline what systems are addressed with patching.

5.11.4 The Organization shall establish procedures for handling exceptions to the patch management process. For instance, situations where some critical systems cannot be taken offline for patching or patching may cause conflicts with other application.

5.12 End User Device Management

5.12.1 Desktop/ Laptop Control

5.12.1.1 Desktop computers shall be connected to UPS to prevent damage of data and hardware.

5.12.1.2 Before leaving a desktop or laptop computer unattended, users shall apply the "Lock Workstation" feature. If not applied, then the device will be automatically locked as per policy of the organization.

5.12.1.3 Confidential or sensitive information that stored in laptops must be encrypted.

5.12.1.4 Desktop computers, laptops, monitors etc. shall be turned off at the end of each workday.

5.12.1.5 Laptops, computer media and any other forms of removable storage containing sensitive information (e.g., CD ROMs, Zip disks, PDAs, Flash drives, external hard- drives) shall be stored in a secured location or locked cabinet when not in use.

5.12.1.6 Access to USB port for Desktop/Laptop computers shall be controlled.

5.12.1.7 Other information storage media containing confidential data such as paper, files, tapes etc. shall be stored in a secured location or locked cabinet when not in use.

5.12.1.8 Individual users must not install or download software applications and/or executable files to any desktop or laptop computer without prior authorization.

5.12.1.9 Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g., virus, worm, Trojan etc).

5.12.1.10 Any kind of abnormal activity or viruses shall be reported immediately.

5.12.1.11 User identification (ID) and authentication (password) shall be required to access all desktops and laptops whenever turned on or restarted.

5.12.1.12 Desktop and laptop computers shall be configured to log all significant computer security relevant events (e.g., password guessing, unauthorized access attempts or modifications to applications or systems software.)

5.12.1.13 All computers shall be placed above the floor level and away from windows.

5.12.1.14 All workstations must be hardened including (but not limited to) the following:

a) Physically securing the workstation and console operations
b) Patching and/or upgrading vulnerable applications and services
c) Eliminating unnecessary services
d) Eliminating programs or services which cause unnecessary security risks or are not used
e) Managing file permissions
f) Establishing restrictions on user accounts and access.

5.12.1.15 All shared resources (e.g., mapped folders, drives, and devices) must have permissions set to allow only those individual accounts or groups that require access

to that resource. These permissions must be reviewed on a regular basis (minimum every 6 months) to ensure appropriate access levels are being maintained.

5.12.2 BYOD Control

5.12.2.1 The Organization shall be aware of the heightened security risks associated with "Bring Your Own Device" (BYOD) due to challenges in securing, monitoring and controlling employees' personal devices.

5.12.2.2 The Organization shall conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.

5.12.2.3 The Organization shall not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks.

5.12.2.4 The Organization may implement appropriate forms of device authentication for PODs approved by authority, such as digital certificates created for each specific device.

5.12.2.5 The Organization has the right to control its information. This must include the right to backup, retrieve, modify, determine access and/or delete organization data without reference to the owner or user of the POD.

5.12.2.6 Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g., using SSL or a VPN).

5.12.2.7 The employee's device shall be remotely wiped if the device is lost or the employee terminates his/her employment or ICT detects a data or policy breach, a virus or similar threat to the security of the bank's data and technology infrastructure.

5.12.2.8 Devices shall be regularly updated.

5.12.2.9 The Organization shall have Mobile device management (MDM) solutions for Managing Devices.

5.12.2.10 The Organization shall restrict installation of application in BYOD as per company policy.

5.12.3 Printer/ Scanner etc. Control

5.12.3.1 The Organization shall take appropriate measures to make sure that office printer/scanner is configured only to allow access from approved networks and devices.

5.12.3.2 The Organization shall change the default password to the administration control panel webpage of Printer/Scanner etc.

5.12.3.3 The Organization shall not allow the organization's printer to store its print history. Many printers like multi-function printers (MFPs) come helpfully equipped with settings that allow users to store print histories or other sensitive information. While that improves speed and performance, it also makes it easy for hackers to swipe if they access the printer.

5.13 Internet of Things (IoT) Control

The Internet of Things (IoT) comprises devices that function as sensors, actuators, controllers, and activity recorders. These devices typically interact with software running elsewhere on the network, such as on a mobile phone, a general-purpose computing device (e.g., a laptop), a machine on the public Internet (e.g., in the cloud), or a combination of these. IoT devices often function autonomously, without requiring human intervention. Thus, ensuring security of IoT devices is one of the most challenging and vital tasks for the organization

5.13.1 The Organization must segregate the network of IoT devices from core network.

5.13.2 The Organization must ensure that all devices connected to the network should be logged and where possible, assessed to determine the level of access they should have.

5.13.3 The Organization must ensure that all the IoT devices are provided with latest software and security patches.

5.13.4 IoT devices shall use strong authentication.

5.13.5 The Organization shall implement standard security best practices for IOT devices which will include but not limited to:

a) Encrypt configuration (Command & Control) communications;
b) Secure communications to and from IoT Controllers;
c) Encrypt local storage of sensitive data;
d) Authenticate communications, software changes, and requests for Data;
e) Use unique credentials for each device;
f) Close unnecessary ports and disable unnecessary services.

5.14 Email Security Management

5.14.1 Email system shall be used according to the organization policy.

5.14.2 Access to email system shall only be obtained through official request.

5.14.3 Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.

5.14.4 Employees must consider the data classification and sensitivity of all email content, before forwarding email or replying to external parties.

5.14.5 Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the organization, or contain any material that is harmful to employees, customers, competitors, or others. The willful transmission of any such material is likely to result in disciplinary action.

5.14.6 The Organization's email system is principally provided for business purposes. Personal use of the email system is only allowed under management discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.

5.14.7 Corporate email address must not be used for any social networking, blogs, groups, forums etc. unless having management approval.

5.14.8 Employees must avoid opening attachments and links for content that is not well understood or looks suspicious. Employees must cross-check the sender information and subject to ascertain their legitimacy

5.14.9 The organization must arrange email security awareness session for all new joiners within 60 days of their enrollment covering the importance of detecting phishing emails, email etiquette and reporting of incidents to appropriate authority within the organization. Organization shall also ensure regular staff communication also covers email security related topic on a regular basis. A yearly refresher of such awareness session is also recommended for all staff for ensuring continuous awareness in this regard.

5.14.10 Email transmissions from The Organization must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

5.14.11 Concerned department shall perform regular review and monitoring of email services.

5.14.12 The Organization shall use end to end encryption (such as PGP) in case of sensitive data transmission.

5.15 Work from Home Management

5.15.1 The Organization shall have an approved Work from Home (WFH) policy.

5.15.2 WFH employees must adhere to the information security policies of the organization at remote work site.

5.15.3 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong passphrases.

5.15.4 All systems that access the organization's networks remotely must have an anti-malware product installed and are kept up to date with latest security updates.

5.15.5 Automatic session logout shall be set for certain time of inactivity.

5.15.6 Employees must ensure the organization's sensitive information must not be readily viewed by unauthorized persons through a window, over a shoulder or by any other means. The employee must also take into cognizance regarding his / her surroundings while discussing official matters over phone while in WFH to prohibit unwanted data leakage.

5.15.7 Employees must not share dynamic password token cards, smart cards, or any other access devices or credentials with anyone.

5.15.8 Employees must keep organizational assets and sensitive documents in a lockable cabinets or desks at home/ remote site.

5.16 Log Management

5.16.1 The Organization shall implement centralized log management system to collect events from multiple sources (servers, networks devices, OS, Database, applications etc.) in a single repository.

5.16.2 A common and accurate time source across the environment shall be used to assure that events from multiple sources can be arranged in an accurate timeline for correlation and analysis.

5.16.3 The Organization shall use correlation across multiple event sources during analysis to improve detection of incidents.

5.16.4 The system event logging should be integrated with the Security Information and Event Management (SIEM) system to in-depth analysis.

5.16.5 Multiple log servers can be deployed to ensure log collection is not interrupted in case of single node failure.

5.16.6 Log data should be archived and retained according to the organization's log retention policy.

Chapter 6: Cyber Security Management

6.1 Threat and Vulnerability Management

6.1.1 The Organization shall establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.

6.1.2 Information about vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

6.1.3 The Organization shall define and establish the roles and responsibilities associated with vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required.

6.1.4 If a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch).

6.1.5 Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:

a) Turning off services or capabilities related to the vulnerability;
b) Adapting or adding access controls, e.g., firewalls, at network borders;
c) Increased monitoring to detect attacks;
d) Raising awareness of the vulnerability.

6.1.6 Define a procedure to address the situation where vulnerability has been identified but there is no suitable countermeasure. In this situation, the organization shall evaluate risks relating to the known vulnerability and define appropriate detective and corrective actions.

6.1.7 The Organization shall address common coding vulnerabilities in software-development processes as follows:

a) Train developers in secure coding techniques, including how to avoid common coding vulnerabilities and understanding how sensitive data is handled in memory;
b) Develop applications based on secure coding guidelines.
Note: Some of the common coding vulnerabilities are listed below:
- Injection flaws, particularly SQL injection
- Buffer overflows
- Insecure cryptographic storage
- Insecure communications
- Improper error handling

- Cross-site scripting (XSS)
- Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)
- Cross-site request forgery (CSRF)
- Broken authentication and session management

6.2 Vulnerability Assessment and Penetration Testing (VAPT)

Vulnerability Assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system.

6.2.1 The Organization shall run internal and external vulnerability scans in the ICT environment periodically and after any significant change in the ICT environment (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

6.2.2 The Organization shall perform at least half yearly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities are resolved. Scans must be performed by qualified personnel.

6.2.3 The Organization shall perform yearly external vulnerability scans for the critical systems/applications, via an independent party. Perform rescans as needed, until satisfactory results are achieved.

6.2.4 For public-facing web applications, the organization shall address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.

6.2.5 Security assessment and testing shall include the following review technique: Documentation Review, Log Review, Rule set Review, System Configuration Review and File Integrity Checking.

6.2.6 Implement a methodology for penetration testing that includes the following:

i) Based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
ii) Includes coverage for the critical systems
iii) Includes testing from both inside and outside the network
iv) Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
v) Specifies retention of penetration testing results and remediation results.

6.2.7 The Organization shall perform internal/external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

6.3 Cryptography

The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is commonly used in Banks and NBFIs to protect sensitive customer information such as PINs relating to critical applications (e.g. ATMs, payment cards and online financial systems).

All encryption algorithms used in a cryptographic solution shall depend only on the secrecy of the key and not on the secrecy of the algorithm. As such, the most important aspect of data encryption is the protection and secrecy of cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys.

6.3.1 The Organization shall encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN or TLS etc. for web-based management and other non-console administrative access.

6.3.2 The Organization shall ensure encryption in 'data at rest' & 'data in transit' for critical data.

6.3.3 The Organization shall establish a procedure on the use, protection, and lifetime of cryptographic keys through their whole lifecycle.

6.3.4 Cryptographic keys must be generated and stored in a secured manner that prevents loss, theft, or compromise. Key generation must be seeded from an industry standard Random Number Generator (RNG). For examples: Approved Random Number Generators for FIPS PUB 140-2.

6.3.5 All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

6.3.6 Keys that are no longer used or needed, or keys that have expired, or keys that are known or suspected to be compromised, should be revoked and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived, encrypted data) they should be strongly protected.

6.3.7 The Organization shall maintain a backup of cryptographic keys.

6.4 Security Incident Management and Monitoring

6.4.1 The Organization shall Create Incident Response Plan. Ensure the plan addresses the following, at a minimum:

- Roles, responsibilities, communication and contact strategies in the event of a compromise
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes

- Analysis of legal requirements for reporting compromises

6.4.2 Review and update the incident response plan at least annually to address system changes or problems encountered during plan implementation, execution, or testing.

6.4.3 The Organization shall have Incident Responding & Handling procedure.

6.4.4 Establish an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication and recovery.

6.4.5 Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training and testing/exercises, and implements the resulting changes accordingly.

6.4.6 The Organization shall establish Incident Monitoring System.

6.4.7 Deploy automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

6.4.8 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls and file-integrity monitoring systems.

6.4.9 Include alerts from critical ICT systems, Databases and Web servers.

6.4.10 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files; and configure the software to perform critical file comparisons.

6.4.11 Monitor and analyze security alerts information and distribute to appropriate personnel.

6.4.12 Designated specific personnel shall be available on a 24/7 basis to review security logs and respond to alerts.

6.4.13 The Organization shall provide Incident Response Training:

a) Provide incident response training to information system users consistent with assigned roles and responsibilities;
b) Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

6.4.15 The Organization shall establish Incident Reporting.

6.4.16 Information security events shall be reported through appropriate management channels as quickly as possible.

6.4.17 The Organization shall establish Security Logging:

a) All hosts and networking equipment must perform security log generation for all components (e.g., OS, service, application).
b) All security events must be logged and must be set to capture significant levels of detail to indicate activity.
c) All workstations must have the ability to transfer logs to a consolidated log infrastructure, if needed.

6.5 Formation of CIRT

6.5.1 The Organization shall form Computer Incident Response Team (CIRT) in order to response immediately on any Cyber Incident Detected in the organization.

6.5.2 CIRT shall follow the following Incident response steps:
i. Preparation
ii. Detection and Analysis
iii. Containment, Eradication and Recovery
iv. Post-Incident Activity

6.5.3 CIRT shall cooperate and report to Bangladesh Bank CIRT and National CIRT.

6.5.4 CIRT shall consist of system administrator, network administrator, database administrator, Middleware application administrator, Application Development manager, Swift Manager and SOC team member, Security experts and Legal Advisor.

6.5.5 The Organization shall arrange necessary training for the CIRT to understand and perform their tasks properly.

6.5.6 CIRT may participate national and international level cyber drill to develop their capacity.

6.6 Threat Intelligence

Threat intelligence or cyber threat intelligence is information an organization uses to understand the threats that have will or are currently targeting the organization. This info is used to prepare, prevent and identify cyber threats looking to take advantage of valuable resources.

6.6.1 The Organization shall introduce Threat Intelligence Platform (TIP) in order to manage threats from all types of sources.

6.6.2 The Organization shall use the threat intelligence feed from different sources, cloud-based threat feed, threat feed from regulatory authority, threat feed from National CIRT etc.

6.6.3 The Organization shall integrate threat feed with Security Information and Event Management (SIEM) data to detect an event and respond accordingly.

6.7 Digital Forensic

6.7.1 The Organization shall arrange for digital forensic setup in order to perform post incident forensic.

6.7.2 The Organization shall train a team to aid professional forensic investigator.

6.7.3 The Organization shall maintain isolation for the affected system during forensic.

6.7.4 The Organization shall ensure the forensic team is not biased.

6.7.5 The Forensic Team shall be aware of the Laws and regulation of the country and perform forensic accordingly.

6.7.6 The Organization shall have proper and adequate setup/tools for forensic operation.

6.7.7 The Forensic Team shall report the investigation to the management and if needed submit report and face the jury in the court.

6.8 Social Engineering

6.8.1 The Organization shall arrange security awareness training for its entire staff in the earliest possible time after the start of employment and annually thereafter. End users should be trained to do the following:

a) Training personnel about identifying social engineering attacks and how to recognize common signs of attack.
b) Defend against phishing attacks
   i) Be suspicious of unexpected email messages or email messages from unknown senders.
   ii) Never open unexpected email attachments.
   iii) Never share sensitive information via email.
   iv) Avoid clicking any link received via email, instant messaging or a social network message.

6.8.2 The staff of the organization shall not share sensitive information with an unauthorized individual.

6.8.3 The Organization shall verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens or generating new keys.

6.8.4 The Organization shall ensure that the staff does not provide personal information or information about their organization, including its structure or networks, unless they are certain of a person's authority to have the information.

6.8.5 The Organization shall enforce Multi-Factor Authentication (MFA) for critical systems.

6.8.6 The Organization shall follow all the controls of ‘Cyber Security Framework’ formulated by Bangladesh Bank.

Chapter 7: Cloud Security Management

Cloud computing holds significant potential to help organizations reduce IT complexity and costs, while increasing agility. Cloud computing is also seen as a means to accommodate business requirements for high availability and redundancy, including business continuity and disaster recovery.

Definition: The National Institute of Standards and Technology (NIST) define cloud computing as follows:
"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models and four deployment models."

Deployment Models:

Deployment models are defined to distinguish between different models of ownership and distribution of the resources used to deliver cloud services. Cloud environments may be deployed over a private infrastructure, public infrastructure or a combination of both. The most common deployment models as per NIST include:

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single Organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public Cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid Cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Service Models: The National Institute of Standards and Technology (NIST) define three types of cloud service model which is as follows:

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

7.1 Governance, Risk and Compliance (GRC)

7.1.1 There shall be a clear strategy for using cloud computing services which is consistent and aligned with organization's overall IT strategy, architecture, risk appetite, level of governance, management comfort and its ability to monitor the cloud service provider.

7.1.2 The Organization shall follow all the controls of the '**Guideline on Cloud Computing**' formulated by Bangladesh Bank.

Chapter 8: Identity and Access Management

The objective of Identity and Access Management (IAM) is to ensure who gets access to what assets at which locations, for how long and for what purpose. The Organization shall only grant access rights and system privileges based on least privileges principle in consistent with job responsibility.

8.1 User Identity and Access Management

8.1.1 The Organization shall define, approve and implement the identity and access management procedure to ensure the segregation of duties including the responsibilities and accountabilities.

8.1.2 The Organization shall review periodically to evaluate the effectiveness of the identity and access management procedure.

8.1.3 Access rights and system privileges shall be granted according to the roles and responsibilities of the official, staff, contractors and service providers.

8.1.4 The Organization shall establish a user access management process to provision, change and revoke access rights to information assets. Access rights shall be authorized and approved by appropriate authority, such as the information asset owner.

8.1.5 For accountability, the organization shall ensure users access and user management activities are uniquely identified and preserve logs for audit and investigation purposes.

8.2 Credential Management

8.2.1 The Organization shall establish a strong password policy and a process to enforce password controls for users' access to IT systems.

8.2.2 The Organization shall implement authentication based on 'what you know', 'what you have' and 'what you are' principle for users with access to sensitive systems to safeguard the critical systems and data from unauthorized access.

8.2.3 The Organization shall ensure that information asset owners perform periodic user access review to justify privileges that are granted to users.

8.2.4 Users shall only be granted access rights to need-to-have basis. Access rights that are no longer required such as change in a user job responsibilities or employment status (e.g. transfer or termination of employment), shall be revoked or disabled immediately.

8.2.5 User access shall be locked for unsuccessful login attempts.

8.2.6 Password controls shall include a change of password upon first logon.

8.2.7 Password length shall be kept minimum eleven characters (In case MFA not used) with the combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers

8.2.8 Maximum validity period of password shall not be beyond the number of days permitted in the organization's Policy (maximum 90 days cycle).

8.2.9 The Organization may use CAPTCHA or similar method to prevent repeated login attempts by intruder.

8.2.10 Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope if Privileges Access Management (PAM) Solution not used.

8.3 Privileged Access Management

Information security ultimately relies on trusting a small group of skilled staff, who shall be subject to proper checks and balances. Their duties and access to systems resources shall be placed under close scrutiny.

8.3.1 The Organization shall apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.

8.3.2 Having privileged access, all system administrators, ICT security officers, programmers and employees performing critical operations invariably possess the capability to inflict severe damage on critical systems. The Organization shall adopt following controls and security practices for privileged users:

i) Implement strong authentication mechanisms;
ii) Implement strong controls over remote access;
iii) Restrict the number of privileged users;
iv) Grant privileged access on a “need-to-have” basis;
v) Review privileged users’ activities on a timely basis;
vi) Prohibit sharing of privileged accounts;
vii) Disallow vendors from gaining privileged access to systems without close supervision and monitoring.

8.4 Remote Access Management

8.4.1 Remote access allows users to connect to the organization’s internal network via an external network to access the organization’s data and systems, such as emails and business applications. Remote connections should be encrypted to prevent data leakage through network sniffing and eavesdropping. Strong authentication, such as multi-factor authentication, should be implemented for users performing remote access to safeguard against unauthorized access to the organization’s ICT environment.

8.4.2 The Organization ensuring remote access to Its information assets shall only be allowed from devices that have been secured according to the organizations security standards.

Chapter 9: Business Resilience

Business Resilience is required for planning of business resiliency for critical incidents; operational risks take into account for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Resilience is to incorporate effective Business Continuity Plan (BCP) that reflects how quickly & effectively restore normal business operations in case of any disaster or other disruptions. In order to survive with minimum financial and reputational loss, the organization shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning. Contingency plan shall also address the backup, recovery and restore process.

9.1 Business Continuity Plan (BCP)

9.1.1 Continuity Planning Policy

9.1.1.1 The Organization shall have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.

9.1.1.2 Approved BCP shall be circulated to all relevant stake holders. The recipients would receive a copy of amended plan whenever any amendment or alteration takes place.

9.1.1.3 Documents related to BCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference.

9.1.1.4 The compliance with the business continuity policy shall be monitored and the effectiveness shall be measured and evaluated.

9.1.1.5 Scope exclusions/deviations for the BCP shall be documented and the justifications for scope exclusions/deviations shall be approved by the senior management.

9.1.1.6 BCP shall address the followings:

a) Action plan to restore business operations within the specified time frame for:
   i) Office hour disaster;
   ii) Outside office hour disaster.

b) Emergency contacts, addresses and phone numbers of employees, support staff, vendors and other relevant agencies;

c) Business Impact Analysis;

d) Disaster recovery site map.

9.1.2 Business Impact Analysis (BIA)

9.1.2.1 The Organization shall define, approve and implement methodologies for BIA, based on Risk Assessment.

9.1.2.2 The Organization shall consider considering people, process, technology and premises while performing BIA.

9.1.2.3 The Organization shall identify and prioritize the activities (i.e., products, services, business functions and processes) by performing BIA to determine the following but not limited to:

a) The potential impact of business disruptions for each prioritized business function and processes, including but not restricted to financial, operational, customer, legal and regulatory impacts
b) The Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs) and Maximum Tolerable Downtime (MTD)

9.1.2.4 The BIA shall be reviewed and updated annually and when major changes occur in the organization (e.g., people, process, technology, suppliers and locations).

9.1.3 Creating Contingency Strategy and Plan

9.1.3.1 Board of directors of the organization shall have the ultimate responsibility for the Business Continuity Management (BCM) program.

9.1.3.2 The board of directors of the organization shall allocate sufficient budget to execute the required BCM activities.

9.1.3.3 The BCM function shall be adequately staffed with qualified team members.

9.1.4 Testing, Training, and Exercises of Plan

9.1.4.1 The tests should consider appropriate scenarios that are well planned with clearly defined objectives (e.g., per function, per service, per process, per location, per worst cases scenarios). The Organization shall take into consideration to include cyber security scenarios.

9.1.4.2 Detailed results of all exercises and tests shall be documented for future reference. The exercises/tests results should include, but not limited to the following considerations:

a) Confirm meeting the objectives of the exercised plan;
b) Confirm capabilities and readiness of recovery resources;
c) Document lessons learnt and the required improvements;
d) In case of failure, Capture the root-cause of the failure and remediation actions should be tracked to successful conclusion.

9.2 Disaster Recovery Plan (DRP)

9.2.1 Disaster Recovery Site (DRS)

9.2.1.1 The Organization shall incorporate Disaster Recovery Plan (DRP) in BCP.

9.2.1.2 The Organization shall establish a Disaster Recovery Site (DRS) which is geographically separated from the primary site (minimum of 10 kilometers radial distance but choice of different seismic zone will be preferred) to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.

9.2.1.3 The DRS location and infrastructure shall be complied with industry standards and

subject to approval from Bangladesh Bank.

9.2.1.4 If Disaster Recovery Site (DRS) is not in different seismic zone, the organization may establish a third site in different seismic zone which will be treated as Disaster Recovery Site (DRS)/Far DC. In such case the DRS in near location will be treated as Near DC and shall be configured accordingly.

9.2.1.5 DRS and/or Near DC shall be equipped with compatible hardware and telecommunication equipment's to support the critical services of the business operation in the event of a disaster.

9.2.1.6 Data, system, network and application configurations, and capacities in the alternative data center should be commensurate to such configurations and capacities maintained in the main data center.

9.2.1.7 The Organization shall test and validate at least annually the effectiveness of DRS and the ability of staff to execute the necessary emergency and recovery procedures.

9.2.1.8 DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test report shall be communicated to management and other stakeholders and preserved for future necessity.

9.2.2 Data Backup and Restore Management

9.2.2.1 The Organization shall develop a data backup and recovery policy in BCP. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- line and off-line backups and the transfer of backups to secure off-site storage.

9.2.2.2 Details of the planned backup schedule for each business application must be created in line with the classification of the application and the information it supports and must specify the type of back-up required (full, partial, incremental, differential, real-time monitoring) at each point in the back-up schedule.

9.2.2.3 The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the business continuity plans for each application.

9.2.2.4 The details of the planned backup schedule for each business application must include the retention period for backed-up or archived information and the retention period must be consistent with local legal and regulatory requirements.

9.2.2.5 All media contained backed-up information must be labeled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content.

9.2.2.6 The backup inventory and log sheet shall be maintained, checked and signed by the supervisor.

9.2.2.7 The Organization shall encrypt backup data in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.

9.2.2.8 The process of restoring information from both on-site and off-site backup storage must be documented.

9.2.2.9 The Organization shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the bank's recovery process.

9.3 Crisis Management

9.3.1 The Organization shall have an approved crisis management plan which may be incorporated in BCP.

9.3.2 The effectiveness of the crisis management plan shall be measured and periodically evaluated.

9.3.3 The Organization shall document a crisis management plan that defines how crisis resulting from major incidents will be addressed and managed, and should include at least:

a) Criteria for declaring a crisis;
b) The Organization should establish a command center for centralized management and an emergency command center;
c) Crisis-management team members: Considering representatives of the critical products, services, functions and processes of the organization (including Communications Department);
d) Contact details of those who are part of the crisis management team (including third parties);
e) Definition of the steps to be taken during and after a crisis or disaster (including the mandates required);
f) Communication plan including the media response plan, to address the communication with the internal and external stakeholders during crisis. The frequency of crisis management tests.

Chapter 10: Acquisition and Development of Information Systems

This chapter covers security discipline of the new software whether it is in development or acquisition with variety of concerns. These concerns are the security of the development environment, software and component security, application security and the secure development lifecycle.

For any new application of business function for The Organization requires rigorous analysis before acquisition or development to ensure that business requirements are met in an effective and efficient manner. This process covers the definition of needs, consideration of alternative sources, review of technological and economic feasibility, execution of risk analysis and cost-benefit analysis and conclusion of a final decision to 'make' or 'buy'.

10.1 Software Documentation

10.1.1 Detailed business requirements and design shall be documented and approved by the competent authority.

10.1.2 System documentation and User Manual shall be prepared and handed over to the concerned department.

10.1.3 Documentation of the software shall be available and safely stored.

10.1.4 Document shall contain the followings:

a) Functionality;
b) Security features;
c) Interface requirements with other systems;
d) System Documentation;
e) Installation Manual;
f) User Manual;
g) Emergency Administrative procedure.

10.2 Separation of Environments

10.2.1 Development, testing and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.

10.2.2 Separate user credentials shall be maintained for Development, testing and production environments.

10.3 In-house Software Development

10.3.1 Rules for the development of software and systems shall be established and applied to developments within the organization.

10.3.2 The Organization shall ensure secure software development processes based on

industry standards and/or best practices like OWASP Development Guide or SANS coding guide etc.

10.3.3 Developed functionality in the application shall be in accordance with design specification and documentation.

10.3.4 Software Development Life Cycle (SDLC) shall be followed and conducted in the development and implementation stage.

10.3.5 Source code must be available with the concerned department and kept secured.

10.3.6 Source code shall contain title area with author name, date of creation, last date of modification and other relevant information.

10.3.7 Ensure processes for code review should at least include the following:

a) Codes are reviewed by individuals other than the original author, who are knowledgeable in code review techniques and in secure coding practices.
b) Code reviews ensure secure coding guidelines (e.g. OWASP) are followed.
c) All custom application code changes are reviewed.

10.3.8 Changes to systems within the development lifecycle shall be controlled using formal change control procedures.

10.3.9 Organization shall establish and appropriately protect environments for secure system development and integration efforts that cover the entire system development lifecycle.

10.3.10 Necessary 'Regulatory Compliance' requirements must be taken into account by the organization.

10.3.11 Similar practices and standards shall be followed for mobile application development.

10.4 Procured Software management

10.4.1 Agreements shall address the information security practices are maintained in vendor institution during development. Following an international standard (e.g. CMMI) is highly recommended.

10.4.2 Agreements shall address the secure transfer of business information between the organization and vendors.

10.5 Software Testing

10.5.1 The testing team of Software/Application/System shall always be separated from the development team.

10.5.2 User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.

10.5.3 User Verification Test (UVT) for post deployment shall be carried out.

10.5.4 Test data shall be selected carefully, protected and controlled.

10.6 Software Security Requirements

10.6.1 Ensure that documented SDLC process includes information security throughout the life cycle.

10.6.2 Testing of security functionality shall be carried out during development.

10.6.3 Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.

10.6.4 During any kind of integration ensure information security throughout the process. Following an international standard is highly recommended.

10.6.5 Only IT personnel will have the privilege to install applications/systems that are authorized and whitelisted by the organization authority.

Chapter 11: Digital Payment Security

Digital Payment is a paradigm shift in the finance and banking sector. Especially the advent of Fintech is an evolution of financial industry. The technology facilitates the customers to avail banking services regardless of physical branch, any specific location or specific time. Customers can perform banking transactions through their ATM, POS, Fintech based apps, access the digital Interactive Voice Response (IVR), Internet Banking etc. Digital Payment ensures higher customer satisfaction at lower operational expenses and transaction costs. However, Security of digital payment is essential to safeguard the customer data and financial activities.

11.1 ATM Transactions

11.1.1 The Organization shall install anti-skimming solutions on ATM devices to detect the presence of unknown devices placed over or near a card entry slot.

11.1.2 The Organization shall install fraud detection mechanisms and send alerts to appropriate staff for follow-up response and action.

11.1.3 The Organization shall implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission.

11.1.4 The Organization shall implement appropriate measures to prevent shoulder surfing of customers' PINs.

11.1.5 The Organization may implement biometric finger vein sensing technology to resist PIN compromise.

11.1.6 The Organization shall conduct video surveillance of activities for 24 hours at these machines (preferably in a centralized system) and maintain the quality of CCTV footage and preserve for at least one year.

11.1.7 The Organization shall confirm transparent or semi-transparent front side of the ATM Booth to make the ATM visible from outside to monitor.

11.1.8 The Organization shall introduce a centralized online monitoring system for Cash Balance, Loading-Unloading functions, Disorders of machine, etc. Cash loading in ATM terminal should ensure dual control.

11.1.9 The Organization shall verify that adequate physical security measures are implemented in ATM devices.

11.1.10 The Organization shall inspect all ATM devices frequently to ensure standard practice (i.e., environmental security for ATM, anti-skimming devices for ATM device surface tempering, etc.) is in place with necessary compliance. Inspection log sheet shall be maintained on ATM booth premises and centrally.

11.1.11 The Organization shall monitor third party cash replenishment vendors' activities constantly and visit third party cash sorting houses regularly. If remote access of vendor is required for support purposes or maintain system components, then safe and secured connectivity must be ensured.

11.1.12 The Organization shall confirm that ATM Terminal OS is updated and hardened as per best practice. BIOS or UEFI should be Password protected.

11.1.13 The Organization shall educate its customers on security measures that are put in place by The Organization and are to maintain by the customers for ATM transactions.

11.2 POS Standards

11.2.1 The Organization shall train and provide necessary manual to its merchants about security practices (e.g. signature verification, device tampering/ replacement attempt, changing default password, etc.) to be followed for POS device handling.

11.2.2 The Organization shall educate its customers on security measures that are put in place by the organization and are to maintain by the customers for POS transactions.

11.2.3 The Organization shall ensure that POS is not storing any confidential information of the card holders' data.

11.2.4 The Organization shall ensure the implementation of EMV Chip-enabled POS or similar latest technology.

11.2.5 The Organization shall implement Point-to-Point Data Encryption for all POS terminals.

11.3 QR Based Transactions

11.3.1 QR based Transactions must be followed by Password/PIN-based authentication

11.3.2 Acquirers and issuers shall comply with relevant circulars issued by Bangladesh Bank regarding Card Present and Card Not Present (CNP) transactions from time to time.

11.3.3 Acquirers shall provide merchant awareness to ensure the presentation of legitimate QR codes.

11.3.4 Issuers shall aware their customers to verify the merchant's name and details while paying through Bangla QR.

11.3.5 For security purposes, issuers shall adopt transaction limits.

11.4 Internet Banking

11.4.1 The Organization shall provide assurance to its customers and users so that online access and transactions performed over the internet are adequately protected and authenticated.

11.4.2 The Organization shall implement a strong password policy including password complexity assessment, periodic enforcement for change of password, blocking account for multiple wrong PIN attempts etc. for Internet Banking customers.

11.4.3 The Organization shall properly evaluate security requirements associated with its internet banking system and adopt mechanisms which are well-established international standards.

11.4.4 The Organization shall formulate Internet Banking Security policy considering technology security aspects as well as operational issues.

11.4.5 The Organization shall ensure that information processed, stored or transmitted between the bank and its customers is accurate, reliable and complete. The Organization shall also implement appropriate processing and transmission controls to protect the integrity of systems and data, e.g. TLS.

11.4.6 The Organization shall implement Multi-Factor Authentication (MFA) for all types of online financial transactions.

11.4.7 An online session needs to be automatically terminated after a fixed period unless the customer is re-authenticated for the existing session to be maintained.

11.4.8 The Organization shall implement monitoring or surveillance systems to follow-up and address subsequently any abnormal system activities, transmission errors or unusual online transactions.

11.4.9 The Organization shall maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). The Organization shall put in place measures to plan and track capacity utilization as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

11.4.10 The Organization shall take appropriate measures to minimize exposure to other forms of attacks such as man-in-the-middle attack (MITMA).

11.5 Payment Cards

11.5.1 The Organization which provides payment card services shall implement adequate safeguards to protect sensitive payment card data. The Organization shall further ensure that sensitive card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission.

11.5.2 The Organization shall ensure that the processing of sensitive or confidential information is done in a secure environment.

11.5.3 The Organization shall perform (not a third-party payment processing service provider) the authentication of customers' sensitive static information, such as PINs or passwords. The Organization shall perform regular security reviews of the infrastructure and processes being used by its service providers.

11.5.4 Equipment used to generate payment card PINs and keys shall be managed in a secured manner. Payment cards and related PINs should send to the customer in a secured manner so that no information can be compromised in transit.

11.5.5 Card personalization, PIN generation, Card distribution, PIN distribution, Card activation groups shall be segregated from each other.

11.5.6 The Organization shall ensure that security controls are implemented at payment card systems and networks. The Organization must comply with the industry security standards, e.g., - Payment Card Industry Data Security Standard (PCI DSS) to ensure the security of cardholder's data.

11.5.7 In case of card personalization by a third party, partner institutions should also be PCI DSS certified with adequate control for communication channel that transmits cardholder's data.

11.5.8 The Organization shall only activate new payment cards upon obtaining both the customer's acknowledgment and call confirmation/OTP verification.

11.5.9 Card must be captured if wrong password will attempt more than three times.

11.5.10 The undelivered and inactivated card should be destroyed in a stipulated period predefined by the organization.

11.5.11 To enhance card payment security, the organization shall promptly notify cardholders via transaction alerts including source and amount for any transactions made on the customers' payment cards.

11.5.12 The Organization shall set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

11.5.13 The Organization shall implement solution to follow up on transactions exhibiting behavior, which deviates significantly from a cardholder's usual card usage patterns. The Organization shall investigate these transactions and obtain the cardholder's authorization prior to completing the transaction.

11.6 Payment Gateway

11.6.1 Payment Gateway Provider shall be PCI-DSS or similar other security standards compliant.

11.6.2 Payment Gateway Provider shall ensure the agreement between them and their respective merchants covering all legal / data breach / cyber incident / regulatory aspects in order to safeguard the interests of the customers.

11.6.3 The Organization shall implement appropriate processing and transmission controls to protect the integrity of systems and data, e.g. TLS.

11.7 Payment Interoperability

11.7.1 The Organization shall operate Payment Interoperability by implementing all security features of digital transactions.

11.7.2 The Organization shall follow a standard data format and the data transmission must be secured by standard method, e.g., TLS.

11.8 Mobile Financial Services

11.8.1 A Policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.

11.8.2 Appropriate risk mitigation measures shall be implemented like transaction limit, transaction frequency limit, fraud checks, AML checks etc. depending on the risk perception, unless otherwise mandated by the regulatory body.

11.8.3 The Organization shall ensure the security of the information accessed, processed or stored at Telecom sites and other services providers.

11.8.4 The Organization shall arrange an agreement with Mobile Network Operator (MNOs) about SIM replacement process which includes sending prior notification and getting confirmation to ensure appropriate measures of MFS account for avoiding risk of unwanted transactions

11.8.5 Services provided by the organization through mobile shall comply with security principles and practices for the authentication of transactions mandated by the regulatory body.

11.8.6 The Organization shall have conformity with 'Regulatory Compliance' requirements of the country.

11.8.7 Proper documentation of security practices, guidelines, methods and procedures used in such mobile financial services shall be maintained and updated.

11.8.8 The Organization shall take appropriate measures so that misconfigured Device cannot access Enterprise Resources and actively deny a device trying to access enterprise data if it is in an insecure state.

11.9 SWIFT System

11.9.1 The Organization shall follow the SWIFT Customer Security Controls Framework (CSCF), which directs the mandatory and advisory security controls for SWIFT users across the financial industry under its Customer Security Program (CSP).

11.9.2 The Organization shall implement the required security controls mentioned in the CSCF by SWIFT, on their own SWIFT infrastructure to ensure tangible security gains and risk reduction.

a) Internet access shall be restricted in SWIFT Servers and related client's PCs;
b) Operator profiles shall be reviewed to check, there are no super key profiles available, admin or monitor profiles do not have message processing rights. Ensure 4 or 6 eye principle is implemented;
c) Multi factor authentication for user sign-on shall be mandatory;
d) Access to be provided only specific ports based on the requirement;
e) Incident response management plan is documented and made aware to each employee of the organization;
f) Define different physical users for different operations and activate checker and maker authentication;

g) Ensure regular update of Security patches (OS & SWIFT application);
h) Implement network/firewall level control i.e. restrict communication to/from SWIFT servers during non-working hours (holidays, after EOD etc.);
i) Passwords need to be kept securely, avoid storing in any of the servers (e.g., notepad or in a document file etc.);
j) Prevent unauthorized physical access to SWIFT servers & sensitive equipment;
k) Restrict USB access for SWIFT Servers & related Client PC's;
l) Conduct scenario-based risk assessment in SWIFT system periodically.

11.9.3 As a requirement under the SWIFT Customer Security Program (CSP), the organization participating in SWIFT must submit an annual Security Attestation to ensure compliance with the required controls.

11.9.4 The independent assessment for the annual SWIFT attestation must be done by a service provider who is enlisted under the Cyber Security Service Provider (CSSP) directory maintained by SWIFT.

11.9.5 The Organization shall conduct assessment based on SWIFT Customer Security Controls Framework (CSCF) by an independent third party (SWIFT enlisted). The assessment shall be performed at least annually.

Chapter 12: Service Provider Management

There is an increasing reliance on external service providers as partners in achieving the growth targets and as effective cost alternatives. ICT outsourcing comes in many forms and permutations. Some of the most common types of ICT outsourcing are in systems development and maintenance, support to DC operations, server/network/storage administration, disaster recovery services, application hosting and hardware maintenance etc.

12.1 Outsourcing

Outsourcing to the different ICT services is a common phenomenon. Agreements of such outsourcing arrangement usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

12.1.1 The Organization seeking to outsource activities shall develop a comprehensive policy for outsourcing duly approved by its Board of Directors.

12.1.2 The Organization shall ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements.

12.1.3 Outsourcing activities shall be evaluated based on the following practices:

a) Objective behind outsourcing;
b) Economic viability;
c) Risks and security concerns;
d) Compliance status of the regulatory guideline(s);
e) Defining the outsourcing strategy.

12.1.4 ICT outsourcing shall not result in any weakening or degradation of the organization's internal controls.

12.1.5 The Organization shall require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

12.1.6 The Organization shall develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include termination plan and identification of additional or alternate technology service providers for such support and services.

12.1.7 The Organization shall have an acquisition plan with the purpose to define the strategy to outsourcing organization selection.

12.1.8 The Organization shall evaluate the specialty of services, quality of support staff and previous reputation of the outsourcing organization.

12.1.9 The Organization shall consider the efficiency, capacity and standard of an

outsourcing organization including work strength of technical resources before finalizing outsourcing company.

12.1.10 The Organization shall ensure that selected outsourcing vendor must be complied of business requirements as well as any other innovative issues for the scratch of the business.

12.1.11 The outsourcing organization shall submit the third party audit report and/or risk assessment report for a specific time interval.

12.1.12 The Organization shall have only outsourced the activities which can be effectively supervised by them and compliance with applicable legal and regulatory requirements can be ensured.

12.2 Service Level Agreement

12.2.1 There shall have Service Level Agreements between the organization and vendors.

12.2.2 The Annual Maintenance Contract (AMC) with the vendor shall be active.

12.2.3 The requirements and conditions covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

12.2.4 Service contracts with all service providers including third-party vendors shall include:

a) Pricing;
b) Measurable service/deliverables;
c) Timing/schedules;
d) Confidentiality clause;
e) Contact person name (on daily operations and relationship levels);
f) Roles and responsibilities of contracting parties including an escalation matrix;
g) Renewal period;
h) Modification clause;
i) Frequency of service reporting;
j) Termination clause;
k) Penalty clause;
l) Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies;
m) Geographical locations covered;
n) Ownership of hardware and software;
o) Documentation (e.g., logs of changes, records of reviewing event logs);
p) Right to have information system audit conducted (internal or external);
q) Information of Sub-Contractor (If any).

12.2.5 Service level agreement will continue to be in-force if the outsourcing to be acquired by or merger with another company. The agreement may have to be negotiated.

12.3 ICT Project Management

12.3.1 In drawing up a project management framework, the organization shall ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, roles and responsibility of staff, definition of project milestones and deliverables.

12.3.2 Project plan for all ICT projects shall be clearly documented and approved. In the project plans, the organization shall set out clearly the deliverables to be realized at each phase of the project as well as milestones to be reached.

12.3.3 During project plan information security requirements shall be considered in the acquisition of new information systems or enhancements to existing ones.

12.3.4 The Organization shall ensure that user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation are approved by the relevant business units and ICT management.

12.3.5 The Organization shall establish management oversight of the project to ensure that milestones are reached and deliverables are realized in a timely manner.

12.4 Vendor Selection for System Acquisition

12.4.1 There must be a core team comprising of personnel from Functional Departments, ICT Departments and Internal Control & Compliance Department, legal Department etc. for vendor selection.

12.4.2 Vendor selection process must have conformity with the Procurement Policy of the organization.

12.4.3 Vendor selection criteria for application must address followings:

a) Market reputation, presence and position in industry;
b) Years in operation;
c) Technology alliances;
d) Extent of customization and work around solutions;
e) Financial strength;
f) Performance and Scalability;
g) Number of installations;
h) Existing customer reference;
i) Support arrangement;
j) Local support arrangement for foreign vendors;
k) Weight of financial and technical proposal;
l) Employee Capabilities;
m) Quality Assurance.

12.5 Cross-border Support Services

12.5.1 The Organization shall provide official authorization/assurance from the group

ensuring the data availability and continuation of services for any circumstances e.g., diplomacy changes, natural disaster, relationship break down, discontinuity of services or others.

12.5.2 The Disaster Recovery Site shall be multi-layered in terms of physical location and redundancy in connectivity.

12.5.3 The Organization shall ensure that the remote access is given to the cross-border service provider following the guidelines mentioned in Chapter 8 of this guideline.

12.5.4 The Organization shall ensure that the support model and relevant service personnel responsibility along with contact details is mentioned within the Service Level Agreement (SLA) with the service provider and only remote access is granted to the relevant personnel as per the SLA. Any deviation must be approved from the appropriate authority & register as an exception in risk register prior to provide any access to the cross-border support.

12.5.5 Prior to any cross-border SLA establishment, the organization shall take necessary approval from Bangladesh Bank considering the Guidelines of outsourcing arrangement.

12.6 Security, Screening and Control

12.6.1 The Organization shall establish a comprehensive outsourcing risk management program for an ongoing monitoring and controlling of all relevant aspects of outsourcing arrangements and procedures guiding corrective actions to be taken when certain events occur.

12.6.2 The board of directors and senior management shall fully understand risks associated with ICT outsourcing. Before appointing a service provider, due diligence shall be carried out to determine its viability, capability, reliability, track record and financial position.

12.6.3 The Organization shall seek to ensure that service providers maintain appropriate ICT security so that information with them and in transit between them and the organization is amply protected.

12.6.4 The Organization shall require the service provider to implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

12.6.5 The Organization shall include appropriate information security, confidentiality, and data protection requirements, as detailed in the Agreement. Agreements with such parties shall be reviewed periodically to validate that information security and data protection requirements remain appropriate.

12.6.6 The Organization shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

12.6.7 Service Provider shall comply with a documented termination or conclusion of service process.

12.6.8 Nondisclosure and confidentiality of the organization Data, including personal

data, shall remain in place following Agreement termination or conclusion.

12.6.9 The Organization shall revoke access to systems and applications storing, allowing access to, or processing organization data promptly upon completion or termination of the Agreement.

12.6.10 The Organization shall maintain a service catalogue for all third party services received preserving up-to-date information of each service rendered, service provider name, service type, SLA expiry date, service receiving manager, service reporting, emergency contact person at service provider, last SLA review date, etc.

12.6.11 Dashboard with significant details (Including components End of Supports, End of Life etc.) for SLAs and AMCs shall be prepared and kept updated.

Chapter 13: Awareness, Education and Training

The security awareness and training program is a critical component of the information security program. It is the vehicle for disseminating security information that the workforce, including managers, need to do their jobs.

These programs will ensure that personnel at all levels of the organization understand their information security responsibilities to properly use and protect the information and resources entrusted to them. Agencies that continually train their workforce in organizational security policy and role-based security responsibilities will have a higher rate of success in protecting information.

13.1 Management

Management Development is essential to the success of the organization in increasing the effectiveness of first level, middle and senior management. The Organization shall introduce training for Management in order to acknowledge:

a) Existing IT Infrastructure & Security Measures;
b) ICT Security related act, policies & guidelines;
c) Responsibilities and Liabilities in case of Security Incident etc.;
d) The role of IT in Business;
e) ICT Governance.

13.2 Employee

13.2.1 The Organization shall select the training delivery method depends on cost-effectiveness in terms of achieving the training outcome. Training activity shall mostly be delivered in a combination of the following forms (individual or corporate):

a) Training provided by internal and/or external experts;
b) On the Job Training (OJT);
c) E-learning;
d) Conferences/Seminars participation;
e) Rotation assignments;
f) Pre-employment training;
g) Training apprentices;
h) Continuous education assistant;
i) Online training;
j) Counseling.

13.2.2 The Organization shall select the training modules based on:

a) Technical Skills: Specialized subjects to develop technical skills and knowledge according to the job/function;

b) Managerial Skills: Skills necessary for employees of managerial levels to manage their function and employees;
c) Soft Skills: To develop personal attributes that enhances an employee's interactions effectively with other employees internally or externally;
d) Professional Certification: Training programs that certify an employee in a certain specialty.

13.3 General User Awareness & Education

13.3.1 The Organization shall arrange Security Awareness and Education for the general user of the organization.

13.3.2 The Organization shall ensure program aims to provide employees the real scenario-based security incident related programs.

13.3.3 The Organization shall arrange Risk Management/Information Security Seminar to increase the level of awareness of employees on risk management and information security on a periodic basis covering all employees by means of either physical or online methods.

13.3.4 The Organization shall ensure adequate training/awareness facilities for IS/ICT Audit team considering any new banking services and technological changes.

13.4 IT Personnel Education and Training

13.4.1 The Organization shall provide professional security training (e.g. Reputed International Community such as ISC2, ISACA, EC-Council, EXIN etc. or Reputed Vendor Certification) for IT Personnel which should be consistent with their work domain.

13.4.2 Professional Training, Certification may be appreciated by reward, incentive, promotion point etc.

13.4.3 The Organization shall provide education for IT Personnel to help understand minimize the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly (reduced need to investigate).

13.4.4 The Organization shall ensure the minimum level of Business Foundation Training for ICT personnel to establish an adequately informed perspective of the Bank's corporate vision, mission, objectives, values, policies, procedures and business strategies.

13.4.5 The Organization shall ensure adequate training/awareness facilities for IS Audit team considering any new banking services and technological changes.

13.5 Training of Trainers (ToT)

13.5.1 The Organization shall provide special training for the internal trainer on a specific topic. Besides, method shall be developed, how a trainer would efficiently

conduct training.

13.5.2 The Organization shall evaluate the qualification and relevant industry experience of the trainer before the appointment for the training program.

13.6 Customer Education

13.6.1 The Organization shall arrange an ICT security awareness-related campaign/program for the customer.

13.6.2 The common objectives of the awareness program will be to:

a) Provide general and specific information about fraud risk trends, types or controls to people who need to know;
b) Help consumers identify areas vulnerable to fraud attempts and make them aware of their responsibilities in relation to fraud prevention;
c) Motivate individuals to adopt recommended guidelines or practices;
d) Create a stronger culture of security with better understanding and commitment;
e) Help minimize the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly (reduced need to investigate).

Chapter 14: Emerging Technology Management

The banking and financial industry in the world is geared up for a transformational space and has gained a significant momentum through embracing futuristic technologies such as applications of Artificial Intelligence (AI), Machine Learning (ML), Data Analytics, Distributed Ledger Technology (e.g. blockchain), Robotics, Cloud computing, etc.

Every technology has a double-edged sword and banks need to carry out due diligence with regard to new technologies since they can potentially introduce additional risk exposures or unintended consequences.

14.1 Artificial Intelligence (AI)

AI helps banks to develop new products according to customer preferences. And, responding to technological developments, many banks are leveraging AI in the front end to smooth customer identification and authentication, mimic live employees through chatbots and voice assistants through voice bots, deepen customer relationships, and provide personalized insights and recommendations.

14.2 AI Security Risks

AI is a relatively new force in business, thus, AI enablers, or the AI itself could create new risks. As well as AI has significant challenges for the organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust.

AI system may have scripting errors, bad algorithm, data difficulties or lapses in data management, technology and process troubles/issues, security snags, inadequate human–machine interactions and may also deliver biased results and underrepresented data population may be used to train the AI model.

14.3 AI Security Controls

The use of AI carries a risk of compliance with protocols related to data privacy, fairness, behavioral risk, personal-identity risk and cyber-security. Thus, appropriate balance between innovation and risk must be enforced by putting in place controls for managing the unimaginable.

14.3.1 Rigorous safeguards shall be ensured so that disgruntled employees or external foes are not be able to corrupt algorithms or use an AI application in malfeasant ways.

14.3.2 Human judgment shall be applied to prove faulty system results or biased results or models misbehavior.

14.3.3 AI models shall be transparent and for improved customer service.

14.3.4 The use of AI system must be continuously monitored & operated by qualified human resources.

14.3.5 Sensitive information like Personally Identifiable Information (PII) may be hidden among anonymized data. Thus, AI system shall be designed in such a way that sensitive information is difficult to reveal (if any).

14.3.6 Employees must be well trained on working knowledge of AI systems, shall have awareness on related risks and mitigation actions.

14.3.7 The Organization shall conduct scenario planning and create a fallback plan to handle disaster situation in case AI model performance drifts, data inputs shift unexpectedly or sudden changes, such as a natural disaster occur in the external environment.

14.4 Machine Learning (ML)

Machine learning for financial forecasting can be applied to many administrative, operational, and client areas of the banking industry. Artificial Intelligence and Machine Learning can provide unprecedented levels of automation, either by taking over the tasks of human experts, or by enhancing their performance while assisting them with routine and repetitive tasks.

Organizations are getting benefitted from machine learning and some common uses are Facial recognition and Optical Character Recognition (OCR) technology.

14.5 ML Security Risks

Machine learning systems open new avenues for attacks that don't exist in conventional procedural programs. One of these is the evasion or adversarial attack, in which a foe attempts to inject inputs to ML models that are intentionally meant to trigger mistakes. The data may look okay to humans, but subtle variances can cause ML algorithms to go wildly off track.

Such attacks may occur at inference time by exploiting the model's internal information, typically in one of two ways like white box attack and black box attack. The most common machine learning attacks are Evasion attacks, Poisoning attacks, Model Inversion attacks, Online System Manipulation, Transfer learning attack and Privacy Attacks.

14.6 ML Security Controls

Following best practices can help fight back the attacks on machine learning systems:

14.6.1 It must be ensured that completely trusted third party or vendor has been involved to train model or provide samples for preparing it.

14.6.2 A mechanism or plan shall be developed to inspect the training data for any

contamination. This should be done if training is done internally.

14.6.3 Ground-truth test shall be performed on the model after every training session. Significant changes in classifications from the original collection will show poisoning.

14.6.4 The model shall be compressed, so it becomes a smooth decision surface resulting in less room for an attacker to manipulate it.

14.6.5 Model shall be trained with all the possible accusatory examples an assailant can use.

14.6.6 Algorithm shall not be biased.

14.7 Data Analytics (DA)

Today, success is achieved by driving intelligent customer engagement based on a data-driven understanding of the business. Technology and digitization have transformed the financial sector by enabling them with real-time actionable insights to make informed decisions, creating competitive advantages and elevating consumer experience. This also allows banks to share potential products, upsells, cross-sells and strategic planning with customers. With AI-backed models, the ability to transform the banking experiences of customers is truly exponential.

14.8 DA Security Risks

Data Tampering, Eavesdropping, Data Theft, Falsifying User Identities, Password related Threats, Unauthorized Access to Tables and Columns or Data Rows and Lack of Accountability are some loopholes of data analytics.

14.9 DA Security Controls

14.9.1 Analyst shall be well versed in all stages of Data Analytics and Data Analysis tools and techniques.

14.9.2 Data Analysts shall monitor the activities related to the systems and user behavior, especially potentially suspicious pattern or behavioral trends, in order to keep threats away.

14.9.3 Tracking of User Access shall be established. In a regular interval, Access should be reviewed.

14.9.4 Sensitive Files shall be quarantined.

14.9.5 Behavior-based permissions shall be established.

14.9.6 Data sanitization shall be in place.

14.9.7 Data Analysts shall report analysis results in a clear and understandable form.

14.10 Robotic Process Automation (RPA)

The volume of unstructured data that banks have to process is growing exponentially with the rise of the digital economy. These are not just banking transaction data, but also other behavior that could allow banks to improve and innovate the customer experience. With a combination of various technologies that enable cognitive and robotic process automation, The Organization can understand customer action and make a judgment at a higher speed, scale and quality. Additionally, smart virtual assistants today are handling transactions, providing important information and helping customers.

Robotic Process Automation is improving the user experience by allowing bots to handle repetitive tasks without human intervention to provide better customer service.

14.11 RPA Security Controls

14.11.1 Accountability for Bot actions must be ensured.

14.11.2 Bot operators and Bot identities must be differentiated.

14.11.3 RPA implementation can lead to an increase in account privileges & fraud. Thus, RPA access shall be strictly restricted to what each bot needs to conduct the assigned task.

14.11.4 RPA tool shall provide complete, system-generated logs without any gaps.

14.11.5 Integrity of the RPA logs shall be protected to aid proper investigation or review in case of RPA security fails or incident happens.

14.11.6 Periodically review and test shall be conducted on RPA scripts with a special focus on business logic vulnerabilities.

14.12 Virtual Meetings & Video Conferencing

Confidential or sensitive Information used during meetings or conference and in meeting rooms available to various groups must be secured and inadvertent disclosure to unauthorized individuals must be ensured.

14.13 Virtual Meetings & Video Conferencing Security Controls

14.13.1 The meeting convener must ensure that any sensitive information on paper or other materials is cleared from the meeting room on completion of the meeting.

14.13.2 All attendees must be made aware by the meeting convener or presenter about their duties on handling of CONFIDENTIAL or SENSITIVE information, which discussed in group meetings.

14.13.3 Encrypted video conferencing facilities must be used for sessions if any CONFIDENTIAL or SENSITIVE information are discussed in the meeting.

14.14 Social Media/Instant Messaging Banking

In recent years, business use of social media has exploded. Many Banks or FOs are using WhatsApp, Facebook, LinkedIn, Viber, Skype and other social media platforms to interact with customers and prospects and to market their products and services. For Banks or FOs, the opportunities these platforms provide also come with significant risks. Social media activity can have a negative impact on The Organization's reputation. The Social media or instant messaging platform must be used for banking so as to maintain suitable information security and protect The Organization's information assets. Uncontrolled and unregulated proliferation of the organization's information may pose significant risk for the organization.

14.15 Social Media Banking Security Controls

14.15.1There must have specific terms & conditions for social media banking.

14.15.2 The Organization must have verified account/profile in an individual social media platform.

14.15.3 Customer must be verified every time through personal/secret questions and/or multifactor authentication/face recognition.

14.15.4 Social media account of the organization never be directly connected with the core/primary systems.

14.15.5 The device from where the official social media account is operated must be dedicated for social media banking and only inevitable software/application will be installed in that device.

14.15.6 Activities and security risks of social media and digital channels must be closely monitored. Continuously watch for phishing links, fraudulent accounts, scams and more shall be ensured.

14.15.7 Sensitive information, customer information shall not be shared through social media account. Employees shall be well trained on what information should or should not be posted or visible to the public.

14.15.8 Malicious URLs and IPs found on social media must be blacklisted/blocked and malicious posts and profiles must be taken down immediately.

14.15.9 Communication/chat history should be safely preserved.

14.16 Distributed Ledger Technology

Distributed ledger or Blockchain technology provides a decentralized, transparent and immutable list of transactions. The Blockchain technology and its applications have been grown rapidly in finance, supply chain, digital identity, energy, healthcare, real estate and government.

The most Blockchain security risks are private key, malware vulnerability, Wallet Attacks, Time jacking Attacks, over 50% Attack, Race attack, Selfish Mining and smart contract.

14.16.1 The Organization shall define and establish a business process and/or procedure in relation of the Blockchain solution and its use cases.

14.16.2 The Organization shall perform the risk management strategy in relation with Blockchain-based solution including but not limited to performing risk assessment and treatment along with on-going monitoring and review.

14.16.3 The Organization shall establish and agree on a process to define the data type that will be stored on the Blockchain along with the data's ownership responsibilities.

14.16.4 The Organization shall define, design, plan, and implement an Identity Access Management (IAM) solution for the granted Blockchain-based service in line with the user on-boarding and off-boarding processes.

14.16.5 The Organization shall establish and agree on the architecture and procedure for Hardware Security Module (HSM) implementation for securing Blockchain identity keys.

14.16.6 The Organization shall protect and secure the internal and external communications of the Blockchain-based solution using a highly secure channel(s).

14.16.7 The Organization should define, develop, implement the security incident and event management process and/or procedure about the Blockchain-based solution including preparation, detection and analysis, containment, eradication, and recovery.

Glossary and Acronyms

2FA	- Two-Factor Authentication
AAA	- Authentication Authorization and Accounting
ACL	- Access Control List
ADC	- Alternative Delivery Channel
AFSS	- Auto Fire Detection & Suppression System
AI	- Artificial Intelligence
AMC	- Annual Maintenance Contract
AML	- Anti-Money Laundering
ATM	- Automated Teller Machine
BCM	- Business Continuity Management
BCP	- Business Continuity Plan
BIA	- Business Impact Analysis
BIOS	- Basic Input/Output System
DLP	- Data Loss Prevention
BRD	- Business Requirement Document
BYOD	- Bring Your Own Device
CAAT	- Computer-Assisted-Auditing Tool
CCTV	- Close Circuit Television
CD ROM	- Compact Disk Read Only Memory
CDs	- Compact Disks
CEO	- Chief Executive Officer
CIO	- Chief Information Officer
CIRT	- Computer Incident Response Team
CISO	- Chief Information Security Officer
CMMI	- Capability Maturity Model Integration
CNP	- Card Not Present
CSCF	- Customer Security Controls Framework
CSP	- Customer Security Program
CSSP	- Cyber Security Service Provider
CSRF	- Cross-Site Request Forgery
CTO	- Chief Technology Officer
DBMS	- Database Management System
DC	- Data Center
DDoS	- Distributed Denial of Service
DMZ	- Demilitarized Zone
DoS	- Denial of Service
DR	- Disaster Recovery
DRP	- Disaster Recovery Plan
DRS	- Disaster Recovery Site

DVD	- Digital Video Disc
E-mail	- Electronic Mail
EMV	- Europay, Mastercard, and Visa
EOD	- End of Day
EPM	-Enterprise Performance Management
FIPS	- Federal Information Processing Standard
GRC	- Governance, Risk, and Compliance
HSM	- Hardware Security Module
IaaS	- Infrastructure as a Service
IAM	- Identity and Access Management
ICC	- Internal Control and Compliance
ICT	- Information and Communication Technology
IDS	- Intrusion Detection System
IoT	-Internet of Things
IP-MAC	-Internet Protocol-Media Access Control
IPS	- Intrusion Prevention System
IS	- Information System
ISACA	- Information Systems Audit and Control Association
ISC2	- International Information System Security Certification Consortium
ISDN	- Integrated Services Digital Network
ICT	- Information and Communication Technology
IVR	- Interactive Voice Response
JD	- Job Description
KRIs	- Key Risk Indicators
LAN	-Local Area Network
MDM	- Mobile Device Management
MFA	- Multi-Factor Authentication
MFPS	- Multi-Function Printers
MITMA	- Man-in-the-Middle Attack
ML	- Machine Learning
MNO	- Mobile Network Operator
MTD	- Maximum Tolerable Downtime
NBFIs	- Non-Bank Financial Institutions
NIST	- National Institute of Standards and Technology
OCR	- Optical Character Recognition
OJT	- On the job training
OS	-Operating System
OTP	- One-Time Password
OWASP	- The Open Web Application Security Project
PaaS	- Platform as a Service
PCI DSS	- Payment Card Industry Data Security Standard
PCs	- Personal Computers
PDA	- Personal Digital Assistant

PGP	- Pretty Good Privacy
PIN	- Personal Identification Number
PODs	- Personally Owned Devices
POS	- Point of Sale
PSO	- Payment System Operator
PSP	- Payment Service Provider
PSTN	- Public Switched Telephone Network
PT	- Penetration Test
QR	- Quick Response
RNG	- Random Number Generator
RPA	- Robotic Process Automation
RPO	- Recovery Point Objective
RTO	- Recovery Time Objective
SANS	-Sysadmin Audit Network And Security
SaaS	- Software as a Service
SDLC	- Software Development Life Cycle
SIEM	- Security Information Event Management
SIM	-Subscriber Identity Module
SLA	- Service Level Agreement
SYSLOG	- System Logging Protocol
SMS	- Short Messaging Service
SOC	- Security Operations Center
SQL	- Structured Query Language
SSL	- Secured Socket Layer
SSID	- Server Set Identifier
SSH	- Secure Shell
SWIFT	- Society for Worldwide Interbank Financial Telecommunications
SWOT	- Strengths, Weaknesses, Opportunities, and Threats analysis
TIP	- Threat Intelligence Platform
TLS	- Transport Layer Security
TOT	- Training of Trainers
TV	- Television
UAT	- User Acceptance Test
UEFI	- Unified Extensible Firmware Interface
UPS	- Uninterrupted Power Supply
USB	- Universal Serial Bus
User ID	- User Identification
URL	- Uniform Resource Locator
UVT	- User Verification Test
UTP	- Unshielded Twisted Pair
VA	- Vulnerability assessment
VLAN	- Virtual Local Area Network
VM	-Virtual Machine
VPN	- Virtual Private Network

WAN	- Wide Area Network
WFH	- Work from Home
WLAN	- Wireless Local Area Network
XSS	- Cross-Site Scripting