ব্যাংকিং প্রবিধি ও নীতি বিভাগ
বাংলাদেশ ব্যাংক
প্রধান কার্যালয়
ঢাকা।
www.bb.org.bd

বিআরপিডি সার্কুলার নং - ১০

তারিখ ঃ ০৫ আষাঢ় ১৪৩০ / ১৯ জুন ২০২৩

ব্যবস্থাপনা পরিচালক/প্রধান নির্বাহী
বাংলাদেশে কার্যরত সকল তফসিলি ব্যাংক।

প্রিয় মহোদয়,

Guideline on ICT Security পরিপালন প্রসংগে।

উপর্যুক্ত বিষয়ে অত্র বিভাগের বিআরপিডি সার্কুলার নং-০৯, তারিখ: সেপ্টেম্বর ১৭, ২০১৫ এর প্রতি দৃষ্টি আকর্ষণ করা যাচ্ছে।

০২। উক্ত সার্কুলারের মাধ্যমে 'Guideline on ICT Security for Banks and Non-Bank Financial Institutions' অনুসরণ/পরিপালন করার জন্য নির্দেশনা প্রদান করা হয়েছিল। ব্যাংকিং খাতে তথ্য ও যোগাযোগ প্রযুক্তির ব্যবহার এবং তথ্য ও যোগাযোগ প্রযুক্তি নির্ভর সেবার পরিধি প্রতিনিয়ত বৃদ্ধি পাচ্ছে। এছাড়া, প্রযুক্তিগত নতুন উদ্ভাবন ব্যাংকিং খাতের ডিজিটাইজেশনকে ত্বরান্বিত করছে। মূলত: প্রতিযোগিতামূলক সুবিধা অর্জনের লক্ষ্যে মানসম্পন্ন ও সাশ্রয়ী ব্যাংকিং সেবা দ্রুততম সময়ে প্রদানের তাগিদে ব্যাংকিং কার্যক্রম আধুনিকায়নে তথ্য ও যোগাযোগ প্রযুক্তির উপর ব্যাংকের নির্ভরশীলতা বাড়ছে। এই নির্ভরশীলতা বৃদ্ধির পাশাপাশি নিরাপত্তা ঝুঁকিও বাড়ছে। উক্ত ঝুঁকি মোকাবেলায় যথোপযুক্ত ব্যবস্থা গ্রহণ করা জরুরী। সার্বিক বিবেচনায়, 'Guideline on ICT Security for Banks and Non-Bank Financial Institutions' পরিমার্জন ও পরিবর্ধনপূর্বক 'Guideline on ICT Security – Version 4.0' প্রণয়ন করা হয়েছে। হালনাগাদকৃত গাইডলাইনটি বাংলাদেশ ব্যাংকের ওয়েবসাইট www.bb.org.bd এ পাওয়া যাবে।

০৩। বর্ণিত অবস্থায়, Guideline on ICT Security – Version 4.0 এর যথাযথ অনুসরণ/পরিপালন করার জন্য নির্দেশনা প্রদান করা হলো।

এ নির্দেশনা অবিলম্বে কার্যকর হবে।

আপনাদের বিশ্বস্ত,

(মোঃ হারুন-অর-রশিদ)
পরিচালক (বিআরপিডি)
ফোন : ৯৫৩০০৯৫

Guideline on ICT Security

Version 4.0, 2023

Bangladesh Bank

Version History

1. Guideline on Information and Communication Technology for Schedule Banks and Financial Institutions - October 2005, Version 1.0
2. Guideline on ICT Security Schedule Banks and Financial Institutions – April 2010, Version 2.0
3. Guideline on ICT Security for Banks and Non-Bank Financial Institutions - May 2015, Version 3.0

Preface

The technology landscape of the financial sector is changing rapidly, and the underlying information technology (IT) infrastructure supporting financial services has grown in size and complexity in recent years. Digital transformation in the financial sector can be characterized by introducing new technologies and using 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 exposure to various 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, infiltrate sensitive financial data or disrupt the IT systems that support financial services. The increasing complexity of information and communication technology (ICT) and consequent security risks have significant adverse impacts on the operations of financial organizations that might negatively affect the customers' interest, the organization's reputation and the nation's economy. Due to the interconnected organizations, IT and security-related incidents risk causing systemic impacts on the financial ecosystem in the long run. The introduction of emerging sustainable technology, formulation of appropriate security policies and practices, development of technology management skills and engagement of the 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 outlines how Banks and Financial Organizations (FOs) should manage the IT and security risks 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 managing IT and security-related risks.

[This page is left blank intentionally]

Technical Committee

Chairman

Debdulal Roy
Executive Director (ICT)
Bangladesh Bank

Members

Khandaker Ali Kamran Al Zahid
Additional Director
Bangladesh Bank

Mohammad Tauhidul Alam
Principle Maintenance Engineer
Bangladesh Bank

Fahad Zaman Chowdhury
Senior Maintenance Engineer and Member Secretary
Bangladesh Bank

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

Nurullah Shahin, PhD
Senior Maintenance Engineer
Bangladesh Bank

Md. Masud Rana
Programmer/Asst.Systems Analyst
Bangladesh Bank

Md. Rakebul Islam Heru
Maintenance Engineer
Bangladesh Bank

Md. Shafiqul Alam
Deputy Director
Bangladesh Bank

Sohel Ahmed
Senior Information Security Officer
Bangladesh Bank

Tuhin Talukder
Assistant Programmer
Bangladesh Bank

Abdullah Al Maruf
Assistant Maintenance Engineer
Bangladesh Bank

Naima Akhter
Deputy General Manager
Sonali Bank Limited

Md. Mamunur Rashid
Deputy General Manager
Bangladesh Krishi Bank

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

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

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

Rahat Azim
AGM and Head of Technology Infrastructure
IDLC Finance Limited

In addition, the following officials also contributed to preparing this guideline:

Muhammad Zakir Hasan, Executive Director (ICT), Bangladesh Bank

Md. Mehedi Hasan, Chief Information Security Officer, Bangladesh Bank

Jayanata Kumar Bhowmick, Senior Systems Analyst, Bangladesh Bank

Mohammad Imtiaz Kabir, Deputy Chief Information Security Officer, Bangladesh Bank

Sumit Kumar, Assistant Maintenance Engineer, Bangladesh Bank

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

Md. Faisal Hossain , FVP and CISO, Mercantile Bank Ltd.

Zahidur Rahman, AVP and Head of IT Security Unit, Southeast Bank Ltd.

Table of Contents

Chapter 1: Introduction

The intricacy of Information and Communication Technology (ICT) and consequent security risks are increasing globally in the financial sector. The frequency of ICT and security-related incidents (including cyber incidents) is rising, with their significant adverse impact on financial organizations' operational activities. Moreover, due to the interconnectedness of financial organizations, ICT security-related incidents risk causing systemic impacts. By formulating this guideline, Bangladesh Bank has described how the supervisor should cover ICT security risks within supervision, how financial organizations should manage to outsource, and the expectations for ICT security management. This guideline outlines how banks and other financial organizations should manage the ICT and security risks they face. In addition, this guidance aims to provide the banks and other financial organizations 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 the Banks, and other financial organizations provide 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 Organization must adhere. The primary objectives of the Guideline are to:

a) Establish ICT Governance in the Financial Sector;
b) Help Organizations develop their own ICT Security Policy;
c) Establish standard ICT Security Management approach;
d) Help Organizations develop secure and reliable ICT infrastructure;
e) Establish a 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 that 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 significant failures of information systems or disasters and ensure timely resumptions;
n) Define 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 and secure usage of emerging technologies.

1.2 Applicability of the Guideline

a) The guideline applies to Bank, Non-bank Financial Institute (NBFI), Mobile Financial Service Providers (MFSP), Payment Service Providers (PSP), Payment System Operator (PSO), White Label ATMs and Merchant Acquirers (WLAMA) and other financial service providers regulated by Bangladesh Bank. All these institutions will be termed "The Organization" throughout this guideline.
b) All activities and operations required 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, digital payment security, 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 and 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 compliance with the ICT security guidelines. A Team/Committee/Entity shall provide the initial observation of any non-compliance issue to the competent authority.

1.3.2 The Organization shall take initiatives to rectify the non-compliance activities 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, the Organization shall seek permission for dispensation from Bangladesh Bank. After the compliance failure multiple times, a penalty may be imposed on the Organization 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 appropriate IT security controls are in place. They must contribute to ICT security planning to ensure that resources, i.e., process and technology, are allocated consistently with business objectives and that sufficient and qualified technical staff are employed. ICT Governance of the Organization includes but is not limited to Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance and Risk coverage fund. The Organization may also introduce different types of personnel verification by the law enforcement agency, including contractors and service providers handling sensitive information.

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 The 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 The 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 to 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 The roles and responsibilities of the ICT Security Committee are (but are 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 shall have an 'ICT Security Policy' that complies with this ICT Security Guideline and be approved by the Board.

2.2.2 The policy shall be reviewed periodically.

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 cases, 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/acknowledgment forms for different ICT requests/operations/services.

2.2.8 The Organization shall have a 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 Organization chart for the ICT departments/divisions.

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

2.3.3 Employees of the ICT departments/divisions/units/sections shall have approved Job Descriptions (JD) with fall back.

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

2.3.5 The Organization shall have user manuals for all applications.

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

2.3.7 The Organization shall analyze to ensure rational distribution of workload to their staff.

2.4 Internal Information System Audit

2.4.1 The Internal Audit/Compliance Department of the Organization shall carry out Internal Information System (IS) audit.

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 a similar automated tools 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 audits shall be done periodically, at least once a year. The audit shall follow a risk-based approach based on the criticality of the services. The report shall be preserved for regulators as and when required.

2.4.6 The Organization shall ensure audit issues are correctly tracked, wholly 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 relevant 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

The Organization shall obtain industry-standard certification in at least a few areas (preferably all), such as Information System Security, ICT Risk Management, Data Center Standard, Quality Management Systems, 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 to mitigate costs of loss or damage of the ICT assets.

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

2.7.3 There shall be a clear policy to use risk coverage funds 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 faced by the Organization include strategic, environmental, market, credit, operational, compliance, etc. In many enterprises, ICT-related risk is considered a component of operational risk. However, even strategic risk can have an ICT component, 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 and Framework

3.1.1.1 The Organization shall establish Risk-aware Culture from 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 through 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. Supply Chain Risk Management ensures the risk associated with relevant suppliers and services providers are well managed and safeguards the Organization from inherent and accidental risks.

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 the ICT Risk Management Framework is documented and continuously improved based on 'lessons learned' during its implementation and monitoring. The ICT risk management framework shall be

approved and reviewed periodically per Organization policy.

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 periodically report the identified ICT security risk status to the ICT Security Committee and Risk Management Committee 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 risk to absorb the loss, e.g., financial loss and reputation damage.

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

3.1.3.3 The Organization shall develop and roll out the ICT risk Tolerance matrix to assess the impact and 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 that require the enterprise to reassess its risk portfolio regularly.

3.1.3.5 The Organization shall define risk factors that influence risk scenarios' frequency or business impact.

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 proper set of KRIs, The Organization shall carry out the following:

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

b) Provide a backward-looking view of 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, business-relevant terms. Effective risk management requires a 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.

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

b) A business person shall understand how ICT-related failures or events can affect critical services and processes.

c) ICT risk assessment shall be done at least once a year to ensure that the Organization's ICT risks are appropriately identified, assessed, and managed.

3.2.1 Risk Identification

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

3.2.1.2 The Organization shall identify each asset's asset owner, custodian and user 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 shall 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 shall be identified to implement adequate controls on assets. Risk analysis should be considered depending on the criticality of assets, the extent of known vulnerabilities, and prior incidents in the Organization.

3.2.2 Risk Analysis

3.2.2.1 The Organization shall perform risk analysis based on qualitative, quantitative, or a combination of both. These include the scale of qualifying attributes to define the 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 the overall risk exposure of the institution.

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

3.2.2.4 The Organization shall establish a business impact analysis 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 developing and using the Risk Scenarios technique to identify the essential and relevant risks. The developed risk scenarios can be used during risk analysis, where the frequency and impact of the scenario are assessed.

3.2.3 Risk Evaluation

3.2.3.1 The Organization shall also develop ICT risk treatment plans in conjunction with the RA to establish necessary compensative controls. This help reduces the identified risk and allows 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 the 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 shall 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 and Control Monitoring

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

3.3.2 The Organization shall define the risk accountability applies to those who own the required resources and have the authority to approve the execution or accept the activity outcome within specific ICT Risk processes. Risk ownership stays with the owner or custodian, whoever is in a 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 The ICT Risk Management Committee shall review and approve risk treatment plans.

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

3.4 Risk Reporting and 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 and control measurement outcome.

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

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

3.5 Risk Communication and Consultation

3.5.1 The Organization shall communicate the identified ICT risk between the responsible division/department and the concerned stakeholders. The communication of ICT risk includes providing assurance of the outcome of the ICT risk management, sharing the results of the ICT risk assessment, support decision-making, improving awareness etc.

3.5.2 The Organization may engage the 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, and new or increased vulnerabilities have been included in the ICT risk management scope;
b) Necessary modification of asset values;
c) ICT security incidents;
d) Configuration, Change Management etc.

[This page is left blank intentionally]

Chapter 4: ICT Service Delivery Management

ICT Service Delivery Management covers the dynamics of technology operation management, including 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 with minimum operational risk.

4.1 Service Request Management

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

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

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

4.1.4 There shall be an 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 the Business Requirements 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 A formal documented process with necessary change details shall govern all changes of business applications implemented in the production environment.

4.2.4 Audit trails shall be maintained for business applications.

4.2.5 The Organization shall prepare a rollback plan for unexpected situations.

4.2.6 User Acceptance Test (UAT) for changes and upgrades in the 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 mishandling that results in a prolonged disruption of ICT services.

4.3.1 The Organization shall establish an incident management framework to restore standard ICT service as quickly as possible following the incident

with minimal impact on 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 Incidents must be accorded the appropriate severity level. As part of the 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 periodically.

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

4.3.6 In some situations, significant 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 if a critical system has failed over its disaster recovery system.

4.3.7 The Organization shall keep customers informed of any significant incident. Maintaining customer confidence throughout a crisis or an emergency 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 incident management aims to restore the ICT service as soon as possible, problem management aims to determine and eliminate the root cause to prevent 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 workflow process to escalate any problem to a concerned person for a quick, effective and orderly response.

4.4.3 Problem findings and action steps will be documented during the problem-resolution process.

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 the 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 has a similar incident occurred over the last two years?
   v. Did detection occur promptly?
   vi. What lessons were learned from this incident?

b) Impact Analysis
   i. The extent of the incident, including information on the systems, resources, and customers that were affected;
   ii. The 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 has to be taken to address the consequences of the incident. Priority shall be placed on addressing customers' concerns.
   ii. Adequate measures shall be taken to address the root cause of the incident.
   iii. Corrective measures shall be taken to prevent similar or related incidents from occurring again.

4.4.6 A trend analysis of past problems shall be performed to identify and prevent similar problems.

4.5 Capacity Management

Capacity management ensures that ICT capacity meets current and future business requirements cost-effectively.

4.5.1 The Organization shall monitor and review performance, capacity and utilization indicators to ensure that ICT systems and infrastructure can support business functions.

4.5.2 The Organization shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to effectively

meet operational and business requirements.

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, considering 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 a 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 arising from the data migration process.
b) Data shall not be manually or electronically altered by a person, or programmer, substituting or overwriting in the new system.
c) The total number of records from the source database is transferred to the new database.
d) The new application shall be consistent/ compatible with 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 after conversion to the new platform separately in the archive for future reference.

4.6.4 The error logs of the pre-migration/ migration/post-migration period, root cause analysis, and action taken must be reviewed immediately.

Chapter 5: Infrastructure Security Management

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

5.1 Asset Management

5.1.1 Asset Acquisition Management

5.1.1.1 Before procuring any new ICT assets, the Organization shall perform compatibility, feasibility, applicability, and availability assessment (with the existing system).

5.1.1.2 All ICT asset procurement shall comply with the procurement policy of the Organization.

5.1.1.3 Each ICT asset shall be assigned to a custodian (an individual or entity) 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 identified and labeled. Labeling shall reflect the established classification of assets.

5.1.2.2 The Organization shall identify all essential information assets and fixed assets and draw up and maintain an ICT asset inventory stating essential 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 shall update the ICT asset inventory periodically.

5.1.2.4 ICT asset inventory shall be adequately protected (preferably using an 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 the production environment shall be subjected to a support agreement with the vendor.

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

5.1.3.4 Use of unauthorized or pirated software shall 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 using portable devices, especially for usage at outside premises.

5.1.4.2 The Organization shall define a policy regarding organizational assets returned 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 shall 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 its 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 a 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.

5.2.1.3 The Organization with a 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, Warm, and Cold sites based on their requirements.

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

a) A hot site is a backup site that is continuously running. It shall allow the Organization to continue normal business operations within a very short period after a disaster. The hot site shall be online and shall be available immediately;
b) The 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) The hot site shall be located far away from the original site to prevent the disaster from affecting the hot site also;
e) Hot site shall be used for business-critical apps;
f) Hot sites may be of two types-
    i) Active-Active: Both sides are alive;
    ii) Active-Passive: Data is replicated in a passive site.

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

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

5.2.1.9 The Organization with a 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 before establishing a new DC/DR or migrating/relocating their existing DC or DR to different locations or entities.

5.2.2 Physical Security

5.2.2.1 The following factors need to be considered before selecting the location of the 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 shall be restricted, and unauthorized access shall be strictly prohibited.

5.2.2.3 Video Surveillance systems shall be capable of capturing individuals, tracking objects and movement and assisting in investigating 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 staff access to the DC shall be revoked 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 an authorized employee in the DC always accompanies visitors.

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 shall be lodged with the purpose of access to 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 using security guards, card access systems, mantraps and surveillance systems where appropriate.

5.2.2.9 An emergency exit door shall be available.

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

5.2.2.11 The manager or a delegate shall maintain an inventory of all computing equipment, associated equipment, and consumables housed in DC.

5.2.2.12 Where an outsourced service supplier operates DC, the contract between the Organization and supplier must indicate that all the policy requirements 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 an outsourced service supplier operates DC, the responsibility for

physical security lies with the supplier. Still, access to such facilities dedicated to using the Organization must be reviewed and authorized.

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

5.2.2.15 The server/network room/rack shall be protected with a lock and key by a responsible person for both the front and back door**.**

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

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

5.2.2.18 The server/network room/rack shall have an appropriate cooling system. Water leakage precautions and a water drainage system from Air Conditioner shall be installed.

5.2.2.19 Data centers shall be protected by building Earthquake Safety guidelines.

5.2.2.20 A power generator shall be in place to continue operations in case of power failure.

5.2.2.21 The fuel of the power generator shall be kept sufficient to meet the demand in case of a national blackout or other similar incidents.

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

5.2.2.23 Immediate measures shall be taken to overload electrical outlets with too many devices.

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

5.2.3 Environmental Security

5.2.3.1 Protection of the Data Center from the risk of damage due to fire, flood, explosion and other forms of disaster shall be designed and applied. Building/Constructing Data Centers and Disaster Recovery Sites in multi-tenant facilitated buildings are discouraged.

5.2.3.2 The layout design of the Data Center, including power supply and network connectivity, shall be adequately 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. A separate storeroom shall be in place to keep all sorts of unused and redundant IT equipment.

5.2.3.5 The sign "No eating, drinking or smoking" and “Emergency Exit” shall be displayed.

5.2.3.6 Dedicated office vehicles for any emergencies shall always be available on-site. Public transport must be avoided while carrying critical equipment

outside the Organization's premises to avoid the risk of any causality.

5.2.3.7 Data Center shall have dedicated telephone communication.

5.2.3.8 The power supply system and other support units shall be separated from the production site and placed in a secure area to reduce the risks from environmental threats.

5.2.3.9 Power supply from the source (Main Distribution Board or Generator) to Data Center shall be dedicated. Electrical outlets from these power sources for any other devices shall 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 contracts shall be on a 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. The wall, ceiling and door of the Data Center shall be fire-resistant.

5.2.4.3 Auto Fire Detection and Suppression System (AFSS) shall be installed and tested periodically. It's essential to have a fire alarm or other fire suppression system in an 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 a 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 shall know how to operate a fire extinguisher.

5.2.4.7 The Organization shall train all personnel serving 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.

5.2.4.10 The Organization may use an eco-friendly fire suppression system.

5.2.4.11 The Organization shall conduct fire drills at least once a year.

5.2.5 Cable Management

5.2.5.1 The Organization shall have a proper cabling management plan.

5.2.5.2 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 IT rack roof cutouts' location and proximity to the vertical cable channels must 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 is 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 color coding standard for each cable type 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 relieve strain at 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 the workload demands of users and customers.

5.2.6.1 The Organization shall conduct a comprehensive inventory of devices, hardware, and software, which includes 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 needs to determine the data center performance metric values they are comfortable with, i.e., how long the Organization store data, what application response times should be, what uptime should be, and so on.

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

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.

5.2.7 Server Room Management

Some of the Organizations have server room apart from Data center or standalone. For this, the following controls shall be applicable:

5.2.7.1 The Organization shall ensure that the Server room (if any) shall have a glass enclosure with a lock and key with a responsible authority.

5.2.7.2 Physical access shall be restricted, and visitor logs shall exist and be maintained for the server room.

5.2.7.3 Access authorization list shall be maintained and reviewed regularly.

5.2.7.4 Server room shall be air-conditioned.

5.2.7.5 Water leakage precautions and water drainage system from Air Conditioner shall be installed.

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

5.2.7.7 UPS shall be in place to provide an uninterrupted power supply to the server.

5.2.7.8 Proper attention shall be given to overloading electrical outlets with too many devices.

5.2.7.9 Channel alongside the wall shall be prepared to allow all the cabling to be in a neat and safe position with the layout of the power supply and data cables.

5.2.7.10 Proper earthling of electricity shall be ensured.

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 fewer or more levels depending on their requirement or the complexity of data management.

5.3.1.4 The Organization shall be aware of Personal Identifiable Information (PII), not to expose it to unintended parties. PII shall only be used if required and with confidentiality.

5.3.2 Data Retention

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

5.3.2.2 The Organization shall ensure a data retention period as per Organization policy. Different data may have different retention periods.

5.3.2.3 The Organization shall delete the data that no longer serve 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 regularly.

5.3.3 Data Custodianship

Data Custodians are responsible for the safe custody, transport, storage of the data and implementation of business rules. 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 a data custodian as per the Organization's policy.

5.3.3.2 The data Custodian shall support to ensure physical security, system security, and safeguard appropriate to the classification level of the data.

5.3.3.3 The data Custodian shall support to ensure disaster recovery plans and facilities are adequate to meet business needs.

5.3.4 Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is detecting and preventing data breaches, infiltration 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, considering 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 and 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 that 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 example, 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 a defined set of privileges.

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

5.4.1.3 Inactive sessions shall expire 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 configuration settings, new patches and service packs before being applied to the production system.

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

5.4.1.7 All unnecessary services running in the production server shall be turned off. Any new services shall not run in the 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 to set limits 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 Systems (OS) shall 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 the 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/turn off unneeded/unused software and services.

5.4.3.2 The Organization shall remove unnecessary system accounts or deactivate guest accounts.

5.4.3.3 The Organization shall make changes (rename, disable, change the 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.

5.4.1.9 The Organization shall implement endpoint security solutions for servers.

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 the 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 Following the approved Internet Access Management Policy, employees will have Internet access.

5.5.1.2 Access to and use of the internet from the Organization's premises shall be secure and not compromise the organization's information security.

5.5.1.3 Access to the Internet from the Organization's premises and systems shall 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 an appropriate authority approves.

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

5.5.1.6 Internet access provided by the Organization must not be used to transact any commercial business activity that the Organization does not do. Personal business interests of staff or other personnel shall not be conducted.

5.5.1.7 Internet access provided by the Organization shall 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 against the personnel involved.

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

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

5.5.1.10 The Organization shall be able to control the Internet-based URL classification/IP reputation and shall have countermeasures for defending against DoS/DDoS attacks.

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.

All the components of remote access solutions, including client devices, remote access servers and internal servers accessed through remote access, should be secured against various 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 shall also ensure that remote access servers are kept with up-to-date patches and 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 remote access levels should be permitted from which types of client 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. A mechanism shall be in place to encrypt and decrypt sensitive data traveling through WAN or public networks.

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 similar measures within internal networks to minimize the impact of security exposures originating from third-party or overseas systems and 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 or Time-based Access Control Lists (ACLs) shall be implemented in the routers to control network traffic.

5.6.1.8 A real-time health monitoring system for infrastructure management shall be implemented to monitor all network equipment and servers.

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

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

5.6.1.11 All unused access switch ports 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 the physical security of all network equipment.

5.6.2.4 The Organization shall use high-quality devices to set up LAN for reliability.

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

5.6.2.6 For remote administration, the secure Login feature (i.e., SSH) shall be enabled in network devices. Any unencrypted login option (i.e., TELNET) shall be

turned off.

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

5.6.2.8 The Organization shall back up and review rules on network security devices regularly 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 the 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 Robust encryption technology shall be utilized if the wireless devices do not support strong encryption for authentication/transmission over wireless networks. In that case, 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 regularly.

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 shall be placed in secure locations with restricted access.

5.6.3.11 The Organization shall review wireless audit logs regularly and maintain that securely on a log server.

5.6.3.12 The Organization shall ensure adequate security of its wireless network and enable monitoring of Rogue devices connected through the wireless network. Any suspicious devices discovered shall be promptly reported to the security team following the incident response plan, process and procedure.

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

5.6.3.14 All personnel shall obtain authorization before utilizing the wireless access point and agree to the liability disclaimer before 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 the storage management network using a firewall or Access Control List (ACL). Management ports, such as serial and console, shall be turned off when unused.

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 impossible.

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

5.7.5 The storage system shall be sufficiently hardened with standard security practices such as turning off 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 shall be configured with a password policy having appropriate complexity. The Organization may enhance the application's security 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 promptly, and known vulnerabilities are remediated as quickly as possible.

5.9 Database Security Management

5.9.1 User accounts and user rights shall be defined. Password and profile policies shall be set up, a strong password 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 and Data rights.

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

5.9.4 A privilege review shall be conducted to identify privileges being used, track the source, and identify privileges not being used.

5.9.5 Access to the database (Containing card data) shall be driven through two-factor authentication.

5.9.6 The database shall not be accessible through the Internet.

5.9.7 The database that stores cardholder data shall be placed in an internal network zone, segregated from the DMZ and other untrusted networks.

5.9.8 A database audit trail must be configured to log the change activity of privileged accounts/end users and sent to a centralized log solution. Role-based Access to DB shall be implemented.

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

5.9.10 Cryptographic Services shall be used to protect and validate critical information at rest and in transit.

5.9.11 The database shall be restored in the test environment for testing backup quality and for practice in case of a disaster in DC.

5.10 Endpoint Security Management

5.10.1 The Organization shall ensure that any private, sensitive or confidential information stored on the 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, and application software will be updated with the latest security-related patches.

5.10.3 OSs that reached the 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 shall be protected by endpoint security protection and running the latest virus definitions to detect the latest viruses and malware accurately.

5.10.5 Disabling or removing endpoint protection or turning off signature definition updates on endpoints is prohibited.

5.11 System Upgrade and Patch Management

5.11.1 The Organization shall establish and ensure that the patch management procedures include identifying, categorizing, and prioritizing. To implement security patches on time, 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 production.

5.11.3 The Organization shall document the patch management procedure. The document shall include scope, roles and responsibilities, timeline, operational 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 critical systems

cannot be taken offline for patching or patching, may cause conflicts with other applications.

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 to 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, the device will be automatically locked as per the policy of the Organization.

5.12.1.3 Confidential or sensitive information that is stored on laptops shall 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 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 ports 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 used.

5.12.1.8 Individual users shall not install or download software applications 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 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.

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

a) Physically securing the workstation and console operations
b) Patching 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) shall have permissions set to allow only those individual accounts or groups that require access to that resource. These permissions shall be reviewed regularly (minimum every six months) to maintain appropriate access levels.

5.12.2 BYOD Control

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

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

5.12.2.3 The Organization shall not proceed with the BYOD implementation if it cannot adequately manage the associated security risks.

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

5.12.2.5 The Organization has the right to control its information, including the right to backup, retrieve, modify, determine access 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 shall 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 their employment, or ICT detects a data or policy breach, a virus or similar threat to the security of the organization'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 the installation of applications in BYOD as per company policy.

5.12.3 Printer/Scanner Controls

5.12.3.1 The Organization shall take appropriate measures to ensure that the 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 the Printer/Scanner etc.

5.12.3.3 The Organization shall ensure adequate controls to secure printers.

5.13 Malicious Code Protection

5.13.1 The environment of the Organization, including servers and workstations, shall be protected from malicious code by ensuring that approved anti-malware solutions are installed.

5.13.2 Files received on electronic media of uncertain origin or unknown networks shall be checked for malicious code before use.

5.13.3 The anti-malware solution shall be updated with the latest virus definition.

5.13.4 Virus auto protection mode shall be enabled to screen disks, tapes, CDs or other media for viruses.

5.13.5 A formal process for managing attacks from malicious code shall include procedures for reporting attacks and recovering from attacks.

5.14 Email Security Management

5.14.1 The email system shall be used according to the Organization's policy.

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

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 shall consider all email content's data classification and sensitivity before forwarding emails or replying to external parties.

5.14.5 Information transmitted by email shall 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 will likely 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’s discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.

5.14.7 Unless management approves, the corporate email address shall not be used for social networking, blogs, groups, forums, etc.

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

5.14.9 The Organization shall arrange an 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 incidents to the

appropriate authority within the Organization. The organization shall ensure regular staff communication also covers email security-related topics regularly. A yearly refresher of such awareness sessions is also recommended for all staff to ensure continuous awareness.

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

5.14.11 The concerned department shall perform regular reviews 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 shall adhere to the organization's information security policies at remote work sites.

5.15.3 Secure remote access shall 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 shall have an anti-malware product installed and be updated with the latest security updates.

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

5.15.6 Employees shall ensure that the organization’s sensitive information shall not be readily viewed by unauthorized persons through a window, over a shoulder or by any other means. The employee shall also take into cognizance their surroundings while discussing official matters over the phone at WFH to prohibit unwanted data leakage.

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

5.15.8 Employees shall keep organizational assets and sensitive documents in lockable cabinets or desks at home/ remote sites.

5.16 Virtual Meetings and Video Conferencing

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

5.16.1 After the meeting completion, the convener shall ensure that any sensitive information on paper or other materials is cleared from the meeting room.

5.16.2 The meeting convener or presenter shall inform all attendees of their duties in handling confidential or sensitive information discussed in group meetings.

5.16.3 Encrypted video conferencing facilities shall be used for sessions if any confidential or sensitive information is discussed in the meeting.

5.17 Log Management

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

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

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

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

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

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

5.18 Cryptography

Cryptography serves various essential purposes in the realm of information security. While cryptography's primary applications are to protect data confidentiality, maintain data integrity, and ensure data authenticity, it also finds extensive use in authentication protocols. Cryptographic digital signatures can be used to verify the authenticity of the data origin and check if the data has been altered. Cryptography is commonly used in the Organization 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. The most critical aspect of data encryption is the protection and secrecy of cryptographic keys, whether master keys, key encrypting keys or data encrypting keys.

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

5.18.2 The Organization shall ensure encryption in 'data at rest' and 'data in transit' for critical data.

5.18.3 Cryptographic keys shall be generated and stored securely to prevent loss, theft, or compromise. Key generation shall be seeded from an industry standard Random Number Generator (RNG).

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

physically protected.

5.18.5 Keys no longer used or needed, expired, or known or suspected to be compromised shall be revoked or destroyed to ensure the keys can no longer be used. They should be strongly protected if such keys need to be kept (for example, to support archived, encrypted data).

5.18.6 The Organization shall maintain a backup of cryptographic keys.

5.18.7 The Organization needs to embrace cryptography standards from reputable international organizations.

5.18.8 The Organization should choose an encryption key length and algorithm that fulfills its security needs and standards.

5.18.9 The Organization should ensure the seed or random number is long enough and random enough when the security of the cryptographic technique depends on its unpredictability.

5.18.10 The Organization should ensure that all cryptographic algorithms have undergone thorough (may be omitted) testing or vetting to verify they match the stated security goals and specifications.

5.18.11 The Organization should monitor cryptanalysis-related advancements and, as needed, update or modify the cryptographic algorithms or lengthen the keys to ensure they can withstand changing threats.

5.18.12 The Organization should establish cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation, and expiry.

5.18.13 After the key is generated, any cryptographic keys or sensitive data used to generate or derive the keys should be safeguarded or safely destroyed.

5.18.14 The Organization should determine the appropriate lifespan of each cryptographic key based on factors such as the data's sensitivity, the system's criticality to be protected, and the threats and risks to which the data or system may be exposed. The cryptographic key should be securely replaced before it expires at its lifespan.

5.18.15 When cryptographic keys are being used or transmitted, the Organization shall ensure that these keys are not exposed during usage and transmission.

5.18.16 When cryptographic keys have expired, the Organization shall use a secure key destruction method to ensure keys could not be recovered by any parties.

5.18.17 When changing a cryptographic key, the Organization shall generate the new key independently from the previous key.

5.18.18 The Organization shall maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys shall be accorded to backup keys.

5.18.19 If a key is compromised, the Organization shall immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. The Organization shall inform all parties concerned about revoking the compromised keys.

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 rating (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 on time. The Organization’s exposure to such vulnerabilities shall be evaluated, and take appropriate measures 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 Suppose a patch is available from a legitimate source. In that case, 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 shall be tested and evaluated before installation to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, alternative 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 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 understand how sensitive data is handled in memory;
b) Develop applications based on secure coding guidelines. Some of the common coding vulnerabilities are listed below:
    i. Injection flaws, particularly SQL injection
    ii. Buffer overflows
    iii. Insecure cryptographic storage
    iv. Insecure communications
    v. Improper error handling
    vi. Cross-site scripting (XSS)

vii. Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)
viii. Cross-site request forgery (CSRF)
ix. Broken authentication and session management
x. Should not use End of Life (EOL) library and resource API.

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 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, and 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 shall be performed by qualified personnel.

6.2.3 The Organization shall perform vulnerability scans for the critical systems/applications once a year by engaging an independent party. The Organization shall have a time-bound remediation plan based on the report.

6.2.4 For public-facing web applications, the Organization shall address new threats and vulnerabilities continuously and ensure these applications are protected against known attacks.

6.2.5 Security assessment and testing may 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 Security Incident Management and Monitoring

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

a) Roles, responsibilities, communication and contact strategies in the event of a compromise
b) Specific incident response procedures
c) Business recovery and continuity procedures
d) Data backup processes
e) Analysis of legal requirements for reporting compromises

6.3.2 The Organization shall review and update the incident response plan annually to address system changes or problems encountered during plan implementation, execution, or testing.

6.3.3 The Organization shall have Incident Responding and Handling procedures.

6.3.4 Establish an incident handling capability for security incidents, including preparation, detection and analysis, containment, eradication and recovery.

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

6.3.6 The Organization shall establish an Incident Monitoring System.

6.3.7 Deploy automated mechanisms to assist in tracking security incidents and collecting and analyzing incident information.

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

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

6.3.10 The Organization shall establish Information Security Operation Center (ISOC)/ Security Operation Center (SOC).

6.3.11 The Organization shall ensure adequate monitoring for unauthorized modification of critical file systems and configuration files or registry.

6.3.12 Monitor and analyze security alert information and distribute it to appropriate personnel.

6.3.13 Designated specific personnel with cyber incident handling capability shall be available on a 24/7 basis to review security logs and respond to alerts.

6.3.14 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 crises.

6.3.15 The Organization shall establish Incident Reporting.

6.3.16 Information security events shall be reported through appropriate management channels quickly.

6.3.17 The Organization shall establish Security Logging:

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

6.4 Formation of CIRT

6.4.1 The Organization shall form a Computer Incident Response Team (CIRT) to respond immediately to any cyber incident detected in the Organization.

6.4.2 CIRT shall follow the following Incident response steps:

a) Preparation
b) Detection and Analysis
c) Containment, Eradication and Recovery
d) Post-Incident Activity

6.4.3 CIRT shall cooperate and report to Bangladesh Bank CIRT.

6.4.4 CIRT shall consist of Subject Matter Experts within Organization that could support CIRT activities.

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

6.4.6 CIRT may participate in national and international cyber drills to develop their capacity.

6.5 Threat Intelligence

Threat intelligence or cyber threat intelligence is information an organization uses to understand the threats that 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.

6.5.1 The Organization shall introduce a Threat Intelligence Platform (TIP) to manage threats from all sources.

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

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

6.6 Digital Forensic

6.6.1 The Organization shall train a team to aid professional forensic investigators.

6.6.2 The Organization shall maintain isolation for the affected system during

forensics.

6.6.3 The Forensic Team shall be aware of the Laws and regulations of the country and perform forensics accordingly.

6.6.4 The Organization shall have proper and adequate knowledge of forensic operations.

6.7 Social Engineering

6.7.1 The Organization shall arrange security awareness training for its entire staff at the earliest possible time after starting employment and annually after that. End users should be trained to do the following:

a) Learn to identify social engineering attacks and recognize common signs of attack.
b) Avoid clicking short code web links and encrypted character web links.
c) Defend against phishing attacks such as
    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.

6.7.2 The staff of the Organization shall not share sensitive information with an unauthorized individual.

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

6.7.4 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 confident of a person's authority to have the information.

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

[This page is left blank intentionally.]

Chapter 7: Cloud Security Management

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

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 comprises five essential characteristics, three service 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 with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more organizations in the community, a third party, or some combination, and it may exist on or off premises.

Public Cloud: The cloud infrastructure is provisioned for unrestricted use by the public. It may be owned, managed, and operated by a business, academic, government organization, or some combination. 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:

Software as a Service (SaaS): The consumer can use the provider's applications on a cloud infrastructure. The applications are accessible from various client devices through 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 individual application capabilities, except for limited user-specific 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 controls 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 can 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 consistent and aligned with the organization's overall IT strategy, architecture, risk appetite, level of governance, management comfort and 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 and follow the country's laws and regulations.

Chapter 8: Identity and Access Management

Identity and Access Management (IAM) ensures 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 the least privileges principle 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 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 an appropriate authority, such as the information asset owner.

8.1.5 For accountability, the Organization shall ensure user access and 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 the "what you know," "what you have," or "who 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 reviews to justify privileges granted to users.

8.2.4 Users shall only be granted access rights on a need-to-have basis. Access rights no longer required, such as a change in a user's 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 the first login.

8.2.7 Password length shall be kept at least eleven characters (In case MFA is not

used) with the combination of at least three stated criteria like uppercase, lowercase, special characters and numbers.

8.2.8 The password's maximum validity period shall not exceed the number of days permitted in the Organization's Policy (maximum 90 days cycle for internal users). For customers, an organization shall setup the validity period per organizational policy.

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

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

8.3 Privileged Access Management

Information security ultimately relies on trusting a group of skilled staff, who shall be subject to proper checks and balances. Their duties and access to systems resources shall be placed under 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 possess the capability to inflict severe damage on critical systems. The Organization shall adopt the 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 secured according to the Organization’s security standards.

8.5 Input Control

8.5.1 The session time-out period for users shall be set following the Organization's Policy.

8.5.2 An audit trail with a User ID and date-time stamp shall be maintained for data insertion, deletion and modification.

8.5.3 Software shall not allow the same user to be both maker and checker of the same transaction unless otherwise permitted by an appropriate authority.

8.5.4 Management approval shall be in place for delegation of authority.

8.5.5 Sensitive data and fields of applications shall be restricted from being accessed.

[This page is left blank intentionally]

Chapter 9: Business Continuity Management

Business Continuity Management (BCM) is required to plan business resiliency for critical incidents; operational risks are considered for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Resilience is to incorporate an effective Business Continuity Plan (BCP) that reflects how quickly and effectively restore normal business operations in case of any disaster or other disruptions. To survive with minimum financial and reputational loss, the Organization shall ensure that critical operations can resume standard processing within a reasonable time frame. The contingency plan shall cover business resumption planning and disaster recovery planning. The 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 the disaster to continue its operation.

9.1.1.2 Approved BCP shall be circulated to all relevant stakeholders. The recipients would receive a copy of the amended plan whenever any amendment or alteration occurs.

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

9.1.1.4 Compliance with the business continuity policy shall be monitored, and effectiveness measured and evaluated.

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

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 people, processes, 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 process, 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 significant changes occur in the Organization (e.g., people, process, technology, suppliers and locations).

9.1.3 Creating a Contingency Strategy and Plan

9.1.3.1 The board of directors of the Organization shall have the ultimate responsibility for the Business Continuity Management (BCM) program.

9.1.3.2 The organization's board of directors shall allocate a 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 be 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 learned and the required improvements;
d) In case of failure, Capture the root cause of the failure and remediation actions should be tracked to a 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 (Preferably in a different

seismic zone) 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 comply with industry standards and be subject to approval from Bangladesh Bank.

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

9.2.1.5 DRS or Near DC shall be equipped with compatible hardware and telecommunication equipment 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 proportional to such configurations and capacities maintained in the primary 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 Scope, Plan Test Result etc. The 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 shall have a planned, scheduled and documented backup strategy involving making online and offline backups and transferring backups to secure off-site storage.

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

9.2.2.3 The frequency of backups taken for information shall 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 shall include the retention period for backup or archived information, and the retention period shall be consistent with legal and regulatory requirements.

9.2.2.5 All media containing backed-up information shall 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 being transported offsite for storage.

9.2.2.8 The process of restoring information from both on-site and off-site backup storage shall 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 Organization's recovery process.

9.3 Crisis Management

9.3.1 The Organization shall have an approved crisis management plan which may be incorporated into 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 crises resulting from major incidents will be addressed and managed and should include at least the following:

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 the 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) The communication plan, including the media response plan, addresses communication with the internal and external stakeholders during a crisis—the frequency of crisis management tests.

Chapter 10: Acquisition and Development of Information Systems

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

Any new business function application for the Organization requires rigorous analysis before acquisition or development to ensure that business requirements are met effectively and efficiently. 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 to the concerned department.

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

10.1.4 A 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 developing 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 or best practices like OWASP Development Guide or SANS coding guide.

10.3.3 Advanced functionality in the application shall follow design specifications and documentation.

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

10.3.5 The source code shall be available with the concerned department and kept secure.

10.3.6 The source code shall contain a title area with the author's name, date of creation, last date of modification and other relevant information.

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

a) Codes are reviewed by individuals other than the original author, knowledgeable in code review techniques and 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 System changes within the development lifecycle shall be controlled using formal change control procedures.

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

10.3.10 The Organization shall consider necessary Regulatory Compliance requirements.

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 that the information security practices are maintained in vendor institutions 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 software/Application/System testing team 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 During any integration, ensure information security throughout the process. Following an international standard is highly recommended.

10.6.4 Only IT personnel will be privileged to install applications/systems authorized and whitelisted by the Organization's authority.

10.7 Statutory Requirements

10.7.1 The User Acceptance Test shall be carried out and signed off by the relevant business units/departments before rolling out in LIVE operation.

10.7.2 Necessary regulatory compliance requirements for banking procedures and practices and relevant laws of the Government of Bangladesh shall be considered.

10.7.3 Any bugs or defects due to design flaws shall be escalated to higher levels in the software vendors' organization and the Organization in time.

10.8 Application Programming Interfaces (APIs) Management

APIs enable various software applications to communicate and interact with each other and exchange data. Open APIs are publicly available APIs that provide developers programmatic access to a software application or web service. The Organization may collaborate with other Organizations (including regulatory bodies) and develop open APIs used by third parties to implement products and services for customers and the marketplace.

10.8.1 The Organization should establish adequate safeguards to manage the development and provisioning of APIs for secure delivery.

10.8.2 A well-defined vetting process should be implemented for assessing third parties' suitability in connecting to the Organization via APIs and governing third-party API access. The vetting criteria should consider factors such as the third party's nature of business, cyber security posture, industry reputation, and track record.

10.8.3 Security standards for designing and developing secure APIs should be established. The standards should include measures to protect the API keys or access tokens, which authorize access to APIs to exchange confidential data. A reasonable timeframe for access token expiry should be defined and enforced to reduce the risk of unauthorized access.

10.8.4 The Organization should implement strong authentication and access control mechanisms to authorize and control access to designated API services.

10.8.5 Strong encryption standards and key management controls should be adopted to secure the transmission of sensitive data through APIs.

10.8.6 A security screening and testing of the API should be performed between the Organization and its third parties before it is deployed into production. The FI should log the access sessions by third parties, such as the identity of the party making the API connections, the date and time, and the data being accessed.

10.8.7 The Organization should implement technologies that provide real-time monitoring and alerting, should be instituted to provide visibility of the usage and performance of APIs, and detect suspicious activities. Robust measures should be established to promptly revoke the API keys or access tokens in case of a breach.

10.8.8 The Organization should ensure adequate system capacity is in place to handle high volumes of API call requests and implement measures to mitigate cyber threats such as denial of service (DoS) attacks.

10.8.9 The Organization shall establish adequate safeguards to manage the development and provisioning of APIs for secure delivery.

10.8.10 A well-defined vetting process shall be implemented for assessing third parties' suitability in connecting to the Organization through APIs and governing third-party API access.

10.8.11 Security standards for designing and developing secure APIs shall be established. The standards should include measures to protect the API keys or access tokens, which authorize access to APIs to exchange confidential data.

10.8.12 A security screening and testing of the API shall be performed between the Organization and its third parties before it is deployed into production.

Chapter 11: Digital Payment Security

Digital Payment is a paradigm shift in the finance and banking sector. The advent of Fintech is an evolution of the financial industry. The technology allows customers to avail banking services regardless of physical branch, location, or 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, digital payment security is essential to safeguard customer data and financial activities.

11.1 ATM/CRM/CDM 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 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), maintain the quality of CCTV footage, and preserve it for at least one year.

11.1.7 The Organization shall confirm the 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 machines, etc. Cash loading in the 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 ATMs, anti-skimming devices for ATM device surface tempering, etc.) is in place with necessary compliance. The 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 and visit third-party cash sorting houses regularly. If remote vendor access is required to support or maintain system components, then safe and

secured connectivity shall be ensured.

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

11.1.13 Anti-malware in ATMs shall be installed. Also, ATMs purchased by the Organization shall be PCI PTS compliant.

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

11.1.15 The Organization shall confirm restricted ATM OS/Application access users with passwords.

11.2 POS Standards

11.2.1 The Organization shall train and provide necessary manuals 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 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 does not store confidential information such as cardholders' 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.

11.2.6 The Organization shall ensure PCI PTS is complied with for the POS terminal.

11.2.7 The Organization shall ensure appropriate security measures for NFC transactions.

11.3 QR Based Transactions

11.3.1 QR-based transactions shall be followed by Password/PIN-based authentication.

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

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

11.3.4 For security purposes, issuers shall adopt transaction limits.

11.4 Internet and App Banking

11.4.1 The Organization shall assure its customers and users 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 password change, blocking accounts 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 that are well-established international standards.

11.4.4 The Organization shall formulate an Internet Banking Security policy considering technology security and operational issues.

11.4.5 The Organization shall ensure that information processed, stored or transmitted between the Organization 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 online financial transactions.

11.4.7 An online session must 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 and supporting systems (such as interface systems, backend host systems and network equipment). The Organization shall implement measures to plan and track capacity utilization and guard against online attacks. These online attacks may include denial-of-service attacks (DoS attacks) and distributed denial-of-service attacks (DDoS attacks).

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

11.4.11 The Organization shall use secure session management techniques to prevent session hijacking, such as generating unique session identifiers, employing secure cookies, and enforcing session timeouts.

11.4.12 The Organization shall employ secure coding practices, such as input validation, output encoding, and secure storage of sensitive data within the application.

11.4.13 The Organization shall regularly perform static and dynamic application security testing (SAST and DAST) to identify and remediate security vulnerabilities in the mobile app code.

11.4.14 The Organization shall perform application hardening (or application shielding) mechanisms. This will protect the app from tampering, misuse, IP theft, and vulnerability exploitation.

11.4.15 The Organization shall implement multiple layers of security controls, including intrusion detection and prevention systems (IDPS), web application firewalls (WAF), and anomaly detection mechanisms to monitor and protect the application against various threats.

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 sensitive or confidential information is processed 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 securely. Payment cards and related PINs should be sent to the customer securely so that no information can be compromised in transit.

11.5.5 Card personalization, PIN generation, Card distribution, PIN distribution, and Card activation groups shall be segregated.

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

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

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

11.5.9 The card shall be captured if the 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 the 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 solutions to follow up on transactions exhibiting behavior that deviates significantly from a cardholder's usual card usage patterns. The Organization shall investigate these transactions and obtain the cardholder's authorization before completing the transaction.

11.6 Payment Interoperability

11.6.1 The Organization shall maintain Payment Interoperability by implementing all security features of digital transactions.

11.6.2 The Organization shall follow a standard messaging/data format, and the data transmission shall be secured using a standard method, e.g., TLS (latest version).

11.7 Mobile Financial Services

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

11.7.2 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.

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

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

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

11.7.6 The Organization shall conform to the country's 'Regulatory Compliance requirements.

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

11.7.8 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.

11.7.9 The Organization should develop a standard architecture based on security

principles, rules, techniques, processes, and patterns to design a secure mobile application.

11.7.10 The auto-complete feature shall be turned off for sensitive information such as login IDs and passwords.

11.7.11 The clipboard/copy-paste function shall be turned off for sensitive data. The Organization may also use an in-app keypad/ keyboard to capture user input.

11.7.12 Mobile apps shall have a proper error-handling mechanism, and all errors shall be logged in the server.

11.7.13 The Organization should ensure that all mobile payments servers and apps related logs are available for audits.

11.7.14 The Organization should ensure notifying users about updates and enforce them within a grace period depending upon the criticality of fixes. The information about fixes may be published in app release notes.

11.7.15 The Organization may ensure that the apps have passed extensive and recursive vulnerability assessment, scan, and intrusion tests to identify weaknesses through internal and independent assessors.

11.7.16 The Organization should ensure to implement of a flexible device registration/binding functionality using multiple properties unique to the device (such as IP address, location, remote server, time of the day, device type, location, PIN code, Wi-Fi information, screen size, browser, etc.) so that only registered devices are allowed to access backend servers.

11.7.17 The device registration/binding shall preferably be implemented using a combination of hardware, software, and service information. In case multiple devices are registered by a user:

a) The user must be notified of every new device registration on the registered mobile number, email, or phone call and

b) The Organization shall maintain a record of all registered.

11.7.18 A login authentication and a risk-based financial-value-based transaction authentication shall be in place.

11.7.19 The Organization should ensure that the initiation of mobile payments, as well as access to sensitive payment and personal data, is protected by robust customer authentication mechanisms, including:

a) Implement multi-factor authentication (MFA) for mobile app user account registration.

b) Robust and configurable PIN/password/pattern or a biometric credential such as face or fingerprint recognition.

c) Time-based one-time passwords (TOTP) for authentication

d) OTP auto-fetching functionality

e) Configure the maximum number of failed authentication attempts, after which access to the mobile payment service is blocked.

f) Define the maximum duration for termination of inactive mobile payment

service sessions.

g) User authentication shall be processed only at the app owner's server end.

h) Ensure that authentication attempts are logged and monitored to detect login anomalies and possible breaches.

11.7.20 The Organization should ensure that sensitive information is not stored in a shared store segment with other apps on mobile devices.

11.7.21 The Organization should ensure that confidential data is deleted from caches and memory after it is used or uninstalled.

11.7.22 The Organization should ensure that the mobile app erases/expire all application-specific sensitive data stored in all temporary and permanent memories of the device during logoff or on termination of the app instance.

11.7.23 The Organization should ensure that a procedure is in place to detect multiple simultaneous login attempts and immediately communicate it to the concerned user through alternate channels such as callback, SMS, email, etc.

11.7.24 The Organization should ensure that the app usage behavior is maintained and monitored through an automated mechanism and may deploy tools to identify any anomaly in the usage and behavior.

11.7.25 The logs shall be stored separately from the application/database servers and protected with appropriate access controls.

11.7.26 The Organization should implement appropriate security safeguards to protect the logs from unauthorized modification or destruction.

11.7.27 The Organization should ensure that all mobile payments servers and apps related logs are available for audits.

11.7.28 The Organization should implement appropriate control to protect transactional data/information against loss or damage.

11.7.29 Server access controls and audit logs shall be maintained at the server level per the data retention policy.

11.8 SWIFT System

11.8.1 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).

11.8.2 The Organization shall implement the 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 PCs;

b) Operator profiles shall be reviewed to check, and no super key profiles are available; admin or monitor profiles do not have message processing rights. Ensure the four or 6-eye principle is implemented;

c) Multi-factor authentication for user sign-on shall be mandatory;
d) Access is to be provided only to specific ports based on the requirement;
e) The 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 updates of Security patches (OS and 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 and sensitive equipment;
k) Restrict USB access for SWIFT Servers and related Client PCs;
l) Conduct scenario-based risk assessments in the SWIFT system periodically.

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

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

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

11.9 Social Media Banking

In recent years, business use of social media has exploded. Many Organizations use WhatsApp, Facebook, LinkedIn, Viber, Skype and other social media platforms to interact with customers and market their products and services. The opportunities these platforms provide for organizations also come with significant risks. Social media activity can harm the Organization's reputation. The uncontrolled and unregulated proliferation of the Organization’s information may pose significant risks for the Organization.

11.9.1 The Organization shall have specific terms and conditions for social media banking.

11.9.2 Activities and security risks of social media and digital channels shall be closely monitored. Continuous monitoring for phishing links, fraudulent

accounts, scams and more shall be ensured.

11.9.3 Malicious URLs and IPs on social media shall be blacklisted/blocked, and malicious posts and profiles shall be taken down immediately.

11.9.4 Only end-to-end encrypted messaging channels, like WhatsApp, shall be used by Organization for providing social media-based banking services.

11.9.5 If the service provider is a foreign organization, the log and report of any customer-level request response (traffic data, content data) shall be explicitly stored by the Organization to ensure the provision of information in case of investigation of any unwanted activities.

11.9.6 The Chabot system shall be hosted on the organization's server to prevent a third party (vendor organization) from accessing the customer's information.

11.9.7 In any unexpected situation, the customer can immediately close the service by contacting the organization's call center.

[This page is left lank intentionally
]

Chapter 12: Service Provider Management

There is an increasing reliance on external service providers as partners in achieving 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 different ICT services is a common phenomenon. Agreements of such outsourcing arrangements 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 all contracting parties' roles, relationships, obligations and responsibilities are fully set out in written agreements.

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

a) The objective behind outsourcing;
b) Economic viability;
c) Risks and security concerns;
d) The 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 that 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 the unavailability of services due to unexpected problems of the technology service provider. This plan may include a termination plan and identification of additional or alternate technology service providers for such support and services.

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

12.1.8 The Organization shall consider the efficiency, capacity and standard of an outsourcing organization, including work strength of technical resources,

before finalizing the outsourcing company.

12.1.9 The Organization shall ensure that the selected outsourcing vendor has complied with business requirements and any other innovative issues for the scratch of the business.

12.1.10 The outsourcing organization shall submit the third-party audit or risk assessment report for a specific time interval.

12.1.11 The Organization shall have only outsourced the activities they can effectively supervise, 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 the following:

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 an information system audit conducted (internal or external);
q) Information of Sub-Contractor (If any).

12.2.5 Service level agreement shall continue to be in force if the outsourcing is to be acquired by or merged 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 responsibilities of staff, and definition of project milestones and deliverables.

12.3.2 The project plan for all ICT projects shall be documented and approved. In the project plans, the Organization shall set out the deliverables to be realized at each project phase and the milestones to be reached.

12.3.3 Information security requirements shall be considered during the project plan to acquire new information systems or enhance existing ones.

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

12.3.5 The Organization shall establish management oversight of the project to ensure milestones are reached and deliverables are realized promptly.

12.4 Vendor Selection for System Acquisition

12.4.1 There shall be a core team comprising personnel from Functional Departments, ICT Departments, Legal Departments etc., for vendor selection.

12.4.2 The vendor selection process shall have conformity with the Procurement Policy of the Organization.

12.4.3 Vendor selection criteria for application shall address the followings:

a) Market reputation, presence and position in the industry;
b) Years in operation;
c) Technology alliances;
d) The extent of customization and workaround 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 breakdown, 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 remote access is given to the cross-border service provider following the controls 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), including Non-Disclosure Agreement (NDA) with the service provider, and only remote access is granted to the relevant personnel as per the SLA. Any deviation shall be approved by the appropriate authority and registered as an exception in the risk register before providing access to cross-border support.

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

12.6 Security, Screening and Control

12.6.1 The Organization shall establish a comprehensive outsourcing risk management program for 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 the risks associated with ICT outsourcing. Before appointing a service provider, appropriate 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 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 requirement remain appropriate.

12.6.6 The Organization shall ensure the equipment does not contain sensitive live data when the service provider takes the hardware for servicing/repair.

12.6.7 The Service Provider shall comply with a documented termination or

conclusion of the service process.

12.6.8 Nondisclosure and confidentiality of the Organization Data, including personal data, shall remain in place following the 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 catalog for all third-party services received, preserving up-to-date information on each service rendered, service provider name, service type, SLA expiry date, service receiving manager, service reporting, emergency contact person at the service provider, last SLA review date, etc.

12.6.11 A dashboard with essential details (Including components End of Supports, End of Life etc.) for SLAs and AMCs shall be prepared and updated.

[This page is left blank intentionally]

Chapter 13: Awareness, Education and Training

The security awareness and training program is critical to the information security program. It is the vehicle for disseminating security information that the workforce, including managers, must 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 success rate in protecting information.

13.1 Management Training

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 to acknowledge the following:

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

13.2 Employee Training

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

a) Training provided by internal 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 the following:

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 enhance an employee's interactions effectively with other employees internally or externally;
d) Professional Certification: Training programs that certify an employee in a specific specialty.

13.3 General User Awareness and Education

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

13.3.2 The Organization shall ensure program aims to provide employees with 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, periodically covering all employees through 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 Reward, incentives, promotion points etc., may appreciate Professional Training and Certification.

13.4.3 The Organization shall provide education for IT Personnel to help understand and 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 Organization'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

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

efficiently conduct training.

13.5.2 The Organization shall evaluate the trainer's qualifications and relevant industry experience 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 with fraud prevention;

c) Motivate individuals to adopt recommended guidelines or practices;

d) Create a more robust 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).

[This page is left blank intentionally]

Chapter 14: Emerging Technology Management

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

Every technology has a double-edged sword, and the Organization must carry out due diligence regarding new technologies since they can potentially introduce additional risk exposures or unintended consequences.

14.1 Artificial Intelligence (AI)

AI helps the Organization to develop new products according to customer preferences. And, responding to technological developments, many organizations 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.

14.1.1 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 organizations, from reputational damage and revenue losses to regulatory backlash, criminal investigation, and diminished public trust.

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

14.1.2 AI Security Management

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, an appropriate balance between innovation and risk must be enforced by putting in place controls for managing the unimaginable.

14.1.2.1 Rigorous safeguards shall be ensured so that disgruntled employees or external foes cannot corrupt algorithms or use an AI application in malfeasant ways.

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

14.1.2.3 AI models shall be transparent for improved customer service.

14.1.2.4 AI systems shall be continuously monitored and operated by qualified human resources.

14.1.2.5 Sensitive information like Personally Identifiable Information (PII) may be hidden among anonymous data. Thus, the AI system shall be designed so that sensitive information is challenging to reveal (if any).

14.1.2.6 "Relevant Employees shall be well trained on working knowledge of AI systems, shall have awareness on related risks and mitigation actions" as all employees may not need working knowledge.

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

14.2 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 benefit from machine learning; some common uses are facial recognition and Optical Character Recognition (OCR) technology.

14.2.1 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 intentionally 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 white and black-box attacks. The most common machine learning attacks are Evasion, Poisoning, Model Inversion, Online System Manipulation, Transfer learning, and Privacy Attacks.

14.2.2 ML Security Management

Following best practices can help fight back the attacks on machine learning systems:
It must be ensured that a completely trusted third party or vendor has been involved in training the model or providing samples for preparing it.

14.2.2.1 A mechanism or plan shall be developed to inspect the training data for contamination when training is done internally.

14.2.2.2 Ground-truth tests shall be performed on the model after every training

session. Significant changes in classifications from the original collection will show poisoning.

14.2.2.3 The model shall be compressed to become a smooth decision surface resulting in less room for an attacker to manipulate it.

14.2.2.4 The model shall be trained with all the possible accusatory examples an assailant can use.

14.2.2.5 The algorithm shall not be biased.

14.3 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. DA also allows the Organizations to share potential products, upsells, cross-sells and strategic planning with customers. With AI-backed models, the ability to transform customers' banking experiences is exponential.

14.3.1 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 in data analytics.

14.3.2 DA Security Management

14.3.2.1 The analyst shall be well-versed in all stages of Data Analytics and Data Analysis tools and techniques.

14.3.2.2 Adequate monitoring may consider the activities related to the systems and user behavior, especially potentially suspicious patterns or behavioral trends, to keep threats away.

14.3.2.3 Tracking of User Access shall be established. At regular intervals, Access should be reviewed.

14.3.2.4 Sensitive Files shall be restricted.

14.3.2.5 Behavior-based permissions shall be established.

14.3.2.6 Data sanitization shall be in place.

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

14.4 Robotic Process Automation (RPA)

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

14.4.1 Accountability for Bot actions shall be ensured.

14.4.2 Bot operators and Bot identities shall be differentiated.

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

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

14.4.5 The integrity of the RPA logs shall be protected to aid proper investigation or review in case RPA security fails or an incident happens.

14.4.6 Periodically review and test shall be conducted on RPA scripts focusing on business logic vulnerabilities.

14.5 Distributed Ledger Technology

Distributed ledger or BlockChain technology provides a decentralized, transparent and immutable list of transactions. Blockchain technology and its applications have increased in finance, supply chain, digital identity, energy, healthcare, real estate and government. Most BlockChain security risks are private key, malware vulnerability, Wallet Attacks, Time jacking Attacks, over 50% Attacks, Race attacks, Selfish Mining and smart contract.

14.5.1 The Organization shall define and establish a business process or procedure concerning the BlockChain solution and its use cases.

14.5.2 The Organization shall perform the risk management strategy concerning Block Chain-based solutions, including but not limited to performing risk assessment and treatment and ongoing monitoring and review.

14.5.3 The Organization shall establish and agree on a process to define the data type stored on the Block Chain along with the data's ownership responsibilities.

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

14.5.5 The Organization shall establish and agree on the architecture and procedure for implementing the Hardware Security Module (HSM) for securing Block Chain identity keys.

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

14.5.7 The Organization should define, develop, and implement the security incident and event management process or procedure about the Block Chain-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 and 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
DDoS	Distributed 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
NDA	Non-Disclosure Agreement
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

PCI-PTS	Payment Card Industry PIN Transaction Security
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
WLAMA	White Label ATM and Merchant Acquirer
WLAN	Wireless Local Area Network
XSS	Cross-Site Scripting

[End]