Guideline on ICT Security
For Banks and Non-Bank Financial Institutions

May, 2015

Version 3.0

Bangladesh Bank

Technical Committee

Chairman

Kazi Nasir Ahmed
Executive Director (ICT)
Bangladesh Bank

Members

Mohammed Ishaque Miah
Senior Systems Analyst
IT Operation & Communication Department
Bangladesh Bank

Manoj Kumar Howlader
Deputy General Manager
Department of Bank Inspection-1
Bangladesh Bank

Md. Motior Rahman
Senior Systems Analyst
Information Systems Development Department
Bangladesh Bank

Jayanta Kumar Bhowmick
Systems Analyst
IT Operation & Communication Department
Bangladesh Bank

Mohammad Imtiaz Kabir
Systems Analyst
IT Operation & Communication Department
Bangladesh Bank

S.M.Tofayel Ahmad
Programmer
IT Operation & Communication Department
Bangladesh Bank

Md. Abdul Jalil
Deputy General Manager
Information Technology Division
Sonali Bank Limited

Muhammad Anwarul Islam
Vice President and Head of IT Security
Eastern Bank Limited

Syed Pear Mahmood
Head of Group Function Technology
Standard Chartered Bank, Bangladesh

Jamshed Atique
Head of IT Operations and Software Delivery
HSBC Bangladesh

Table of Contents

[This page is intentionally left blank.]

Chapter 1

1. Introduction

The banking industry has changed the way of providing services to their customers and processing of information in recent years. Information and Communication Technology (ICT) has brought this momentous transformation. Electronic banking is becoming more popular and enhancing the adoption of financial inclusion. Security of Information for financial institutions has therefore gained much importance and it is vital for us to ensure that the risks are properly identified and managed. Moreover, information and information technology systems are essential assets for the Banks and Non-Bank Financial Institutions (NBFIs) as well as for their customers and stakeholders. Information assets are critical to the services provided by the Banks and NBFIs to their customers. Protection and maintenance of these assets are important to the organizations' sustainability. Banks and NBFIs must take the responsibility of protecting the information from unauthorized access, modification, disclosure and destruction. Approaches of Banks and NBFIs for business leading to services are risk-based, which means ICT risk is also associated with banking system that needs to be managed with thoughts and efforts.

This revised version of Guideline on ICT Security for Banks and NBFIs is to be used as a minimum requirement and as appropriate to the level of technology adoption of their operations.

1.1 Objectives

This Guideline defines minimum control requirements to which each Bank or NBFI must adhere. The primary objectives of the Guideline are:

a) To establish a standard ICT Security Policy and ICT Security Management approach
b) To help the Banks and NBFIs for secured setup of its ICT infrastructure
c) To establish a secured environment for the processing of data
d) To establish a holistic approach for ICT Risk management
e) To establish a procedure for Business Impact Analysis in conjunction with ICT Risk Management
f) To aware stakeholders' roles and responsibilities for the protection of information
g) To prioritize information and ICT systems and associated risks those need to be mitigated
h) To establish appropriate project management approach for ICT projects

i) To aware and train the users associated with ICT activities for achieving the business objectives
j) To define procedure for periodic review of the policy
k) To ensure the best practices (industry standard) of the usage of technology that is not limited to this guideline
l) To analyze security risks against faster adoption of Bring-Your-Own-Devices (BYOD)
m) To minimize security risks for electronic banking infrastructure including ATM and POS devices, payment cards, internet banking, mobile financial services, etc.

1.2 Applicability of the Guideline

This ICT Security Guideline is a systematic approach of controls to policies required to be formulated for ensuring security of information and ICT systems. This Guideline covers all information that are electronically generated, received, stored, replicated, printed, scanned and manually prepared. The provisions of this Guideline are applicable for:

a) Banks and NBFIs for all of their Information Systems.
b) All activities and operations required to ensure data security including facility design, physical security, application security, network security, ICT risk management, project management, infrastructure security management, service delivery management, disaster recovery and business continuity management, alternative delivery channels management, acquisition and development of information systems, usage of hardware and software, disposal policy and protection of copyrights and other intellectual property rights.

1.3 Categorization of Banks and NBFIs

Depending on the architecture of core business application solution, ICT infrastructure, operational environment and procedures, a Bank or NBFI can be categorized as follows:

Category-1: Centralized ICT Operation for managing core business application solution through Data Center (DC) with backup assets for continuation of critical services including Disaster Recovery Site (DRS)/Secondary Data Center to which all other offices, branches and booths are connected through WAN with 24x7 hours attended operation.

Category-2: Decentralized ICT operation for managing distributed business application solution hosted at DC or operational offices/branches with backup assets for continuation of critical services connected through WAN or having standalone operations.

Chapter 2

2. ICT Security Management

ICT Security Management must ensure that the ICT functions and operations are efficiently and effectively managed. Banks and NBFIs shall be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and risks of possible abuses. They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial transactions and reporting. They have to contribute in ICT security planning to ensure that resources are allocated consistent with business objectives and to ensure that sufficient and qualified technical staffs are employed so that continuance of the ICT operation area is unlikely to be seriously at risk. ICT Security Management deals with Roles and Responsibilities, ICT Security Policy, Documentation, Internal and External Information System Audit, Training and Awareness, Insurance or Risk coverage fund.

2.1 Roles and Responsibilities

Well-defined roles and responsibilities of Board and Senior Management are critical while implementing ICT Governance but clearly-defined roles enable effective project control and expectations of organizations. ICT Governance stakeholders include Board of Directors, CEO, ICT Steering Committee, ICT Security Committee, CIO, CTO, CISO, Risk Management Committee, Chief Risk Officer and Business Executives.

2.1.1 Roles and responsibilities of Board of Directors

a) Approving ICT strategy and policy documents.
b) Ensuring that the management has placed an effective planning process.
c) Endorsing that the ICT strategy is indeed aligned with 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 and acceptable budgets.
f) Ensure compliance status of ICT Security Policy.

2.1.2 Roles and responsibilities of ICT Steering Committee

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

a) Monitor management methods to determine and achieve strategic goals
b) Aware about exposure towards ICT risks and controls
c) Provide guidance related to risk, funding, or sourcing
d) Ensure project priorities and assessing feasibility for ICT proposals
e) Ensure that all critical projects have a component for "project risk management"
f) Consult and advise on the selection of technology within standards
g) Ensure that vulnerability assessments of new technology is performed
h) Ensure compliance to regulatory and statutory requirements
i) Provide direction to architecture design and ensure that the ICT architecture reflects the need for legislative and regulatory compliance

2.1.3 Roles and responsibilities of ICT Security Committee

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

a) Ensure development and implementation of ICT security objectives, ICT security 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 ICT risk management framework/process and to establish acceptable ICT risk thresholds/ICT risk apatite 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 Each Bank or NBFI must have an 'ICT Security Policy' complied with this ICT Security Guideline and be approved by the board.

The policy covers common technologies such as computers and peripherals, data and network, applications and other specialized ICT resources. Banks' service delivery depends on availability, reliability and integrity of its information

technology system. Therefore, each Bank or NBFI must adopt appropriate controls to protect its information system. The senior management of the Bank or NBFI must express commitment to ICT security by ensuring continuous awareness and training program for each level of staff and stakeholders.

2.2.2 The policy requires regular update to deal with evolving changes in the ICT environment both within the Bank or NBFI and overall industry.

2.2.3 Bank or NBFI shall engage ICT security professional employed in separate ICT security department/unit/cell for improved and impartial dealing with security incidents, policy documentation, inherent ICT risks, risk treatments and other relevant activities.

2.2.4 For noncompliance issues, compliance plan shall be submitted to Bangladesh Bank for taking dispensation. Dispensation shall be for a specific period of time.

2.3 Documentation

2.3.1 Bank or NBFI shall have updated organogram for ICT department/division.

2.3.2 Bank or NBFI shall have ICT support unit/section/personnel (Business/ICT) in the branch organogram.

2.3.3 Each individual within ICT department/division/unit/section shall have approved Job Description (JD) with fallback resource person.

2.3.4 Bank or NBFI shall maintain segregation of duties for ICT tasks.

2.3.5 Bank or NBFI shall maintain detailed design document for all ICT critical systems/services (e.g. Data Center design, Network design, Power Layout for Data Center, etc.).

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

2.3.7 Bank or NBFI shall maintain 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).

2.3.8 Bank or NBFI shall have approved relevant requisition/acknowledgement forms for different ICT request/operation/services.

2.3.9 Bank or NBFI shall have User Manual of all applications for internal/external users.

2.4 Internal Information System Audit

2.4.1 Internal Information System (IS) audit shall be carried out by Internal Audit Department of the Bank or NBFI.

2.4.2 Internal IS audit shall be conducted by personnel with sufficient IS Audit expertise and skills. Engagement of certified IS auditor having adequate audit experience in this area of technology will be appreciated.

2.4.3 Bank or NBFI may use Computer-Assisted-Auditing Tools (CAATs) to perform IS audit planning, monitoring/auditing, control assessment, data extraction/ analysis, fraud detection/prevention and management.

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

2.4.5 Internal Information System audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required. Bank or NBFI shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

2.4.6 The bank/branch or NBFI shall take appropriate measures to address the recommendations made in the last Audit Report (external/internal). This must be documented and kept along with the Audit Report mentioned in 2.4.5.

2.5 External Information System Audit

2.5.1 Bank or NBFI may engage external auditor(s) for their information systems auditing in-line with their regular financial audit.

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

2.6 Standard Certification

2.6.1 Bank or NBFI may obtain industry standard certification related to their Information System Security, Quality of ICT Service Delivery, Business Continuity Management, Payment Card Data Security, etc.

2.7 Security Awareness and Training

2.7.1 As technology evolves rapidly, Bank or NBFI shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.

2.7.2 Bank or NBFI shall also ensure the minimum level of Business Foundation Training for ICT personnel.

2.7.3 Bank or NBFI shall arrange security awareness training/workshop for all staff.

2.7.4 Bank or NBFI shall ensure adequate training/awareness facilities for IS Audit team considering any new banking services and technological changes.

2.8 Insurance or Risk Coverage Fund

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

2.8.2 The risk coverage fund shall be maintained properly in the accounting system of Bank or NBFI, if applicable.

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

Chapter 3

3. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Other risks Bank or NBFI faces include strategic risk, environmental risk, market risk, credit risk, operational risk, compliance risk, etc. In many enterprises, ICT related risk is considered to be a component of operational risk. However, even strategic risk can have an ICT component itself, especially where ICT is the key enabler of new business initiatives. The same applies for 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 business risk - specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of ICT within a Bank or NBFI. It consists of ICT related events and conditions that could potentially impact the business. It can occur with both uncertain frequency and magnitude and it creates challenges in meeting strategic goals and objectives.

3.1 ICT Risk Governance

3.1.1 The Bank or NBFI shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.

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

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

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

3.1.5 The Bank or NBFI shall define the risk responsibilities to individuals for ensuring successful completion.

3.1.6 The Bank or NBFI shall define the risk accountability applies to those who owned the required resources and have the authority to approve the execution and/or accept the outcome of an activity within specific ICT Risk processes. Ownership

of risk stays with owner or custodian whoever is in better position to mitigate the identified risk for that specific ICT asset.

3.1.7 The Bank or NBFI shall acknowledge all risks by *Risk Awareness* so that those are well understood and known and recognized as the means to manage them.

3.1.8 The Bank or NBFI shall contribute to executive management's understanding of the actual exposure to ICT risk by *Open Communication,* enabling definition of appropriate and informed risk responses.

3.1.9 The Bank or NBFI shall aware amongst all internal stakeholders of the importance of integrating risk and opportunity in their daily duties.

3.1.10 The Bank or NBFI shall be transparent to external stakeholders regarding the actual level of risk and risk management processes in use.

3.1.11 The Bank or NBFI shall begin *Risk-aware Culture* from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

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

3.2 ICT Risk Assessment

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

a) An 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 key services and processes.

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

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

3.2.3 The Bank or NBFI shall define *Risk Factors* those influence the frequency and/or business impact of risk scenarios.

3.2.4 The Bank or NBFI shall interpret risk factors as casual factors of the scenario that is materializing, or as vulnerabilities or weaknesses.

3.2.5 ICT security department/unit/cell shall conduct periodic ICT risk assessment of ICT related assets (process and system) and provide recommendation to risk owners for mitigation.

3.3 ICT Risk Response

Risk response is to bring measured risk in line with the defined risk tolerance level for the organization. In other words, a response needs to be defined such that as much future residual risk as possible (usually depending on budgets available) falls within risk tolerance limits. When the analysis shows risks deviating from the defined tolerance levels, a response needs to be defined. This response can be any of the four possible ways such as Risk Avoidance, Risk Reduction/Mitigation, Risk Sharing/Transfer and Risk Acceptance.

3.3.1 The Bank or NBFI 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).*

3.3.2 The Bank or NBFI shall give effort to implement, measure and report different indicators that are equivalent in sensitivity.

3.3.3 Selection of the right set of KRIs, Bank or NBFI shall carry out:

a) Provide an early warning for a high risk to take proactive action
b) Provide a backward-looking view on risk events that have occurred
c) Enable the documentation and analysis of trends
d) Provide an indication of the risk's appetite and tolerance through metric setting
e) Increase the likelihood of achieving the strategic objectives
f) Assist in continually optimizing the risk governance and management environment

3.3.4 The Bank or NBFI shall define risk response to bring risk in line with the defined risk appetite for the Bank or NBFI after risk analysis.

3.3.5 The Bank or NBFI shall strengthen overall ICT risk management practices with sufficient risk management processes.

3.3.6 The Bank or NBFI shall introduce a number of control measures intended to reduce either of an adverse event and/or the business impact of an event.

3.3.7 The Bank or NBFI shall share or reduce risk frequency or impact by transferring or otherwise sharing a portion of the risk, e.g. insurance, outsourcing.

Chapter 4

4. ICT Service Delivery Management

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

4.1 Change Management

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

4.1.2 Bank or NBFI shall prepare Business Requirement Document (BRD) which will cover the requirements of system changes and the impact that will have on business processes, security matrix, reporting, interfaces, etc.

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

4.1.4 Audit trails shall be maintained for business applications.

4.1.5 Bank or NBFI shall prepare rollback plan for unexpected situation.

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

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

4.2 Incident Management

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

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

4.2.2 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, the Bank or NBFI may delegate the function of determining and assigning incident severity levels to a technical helpdesk

function. The Bank or NBFI 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.

4.2.3 The Bank or NBFI shall establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident.

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

4.2.5 The Bank or NBFI shall form an *ICT Emergency Response Team*, comprising staff within the Bank or NBFI with necessary technical and operational skills to handle major incidents.

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

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

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

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

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

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

iii. Breach of regulatory requirements and conditions as a result of the incident.

c) Corrective and Preventive Measures

i. Immediate corrective action to be taken to address consequences of the incident. Priority shall be placed on addressing customers' concerns.

ii. Measures to address the root cause of the incident.

iii. Measures to prevent similar or related incidents from occurring.

4.2.10 The Bank or NBFI shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

4.3 Problem Management

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

4.3.1 Bank or NBFI shall establish a process to log the information system related problems.

4.3.2 The Bank or NBFI shall have the process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.

4.3.3 Problem findings and action steps taken during the problem resolution process shall be documented.

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

4.4 Capacity Management

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

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

4.4.2 The Bank or NBFI shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and business requirements effectively.

Chapter 5

5. Infrastructure Security Management

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

5.1 Asset Management

5.1.1 Prior to procuring any new ICT assets, compatibility assessment (with existing system) shall be performed by the Bank or NBFI.

5.1.2 All ICT asset procurement shall be complied with the procurement policy of Bank or NBFI.

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

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

5.1.5 Bank or NBFI shall maintain an ICT asset inventory stating significant details (e.g. owner, custodian, purchase date, location, license number, configuration, etc.).

5.1.6 Bank or NBFI shall review and update the ICT asset inventory periodically.

5.1.7 Information system assets shall be adequately protected from unauthorized access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

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

5.1.9 Bank or NBFI shall provide guidelines for the use of portable devices, especially for the usage at outside premises.

5.1.10 Bank or NBFI shall provide policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.

5.1.11 Bank or NBFI 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.

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

5.1.13 Bank or NBFI shall approve list of Software which will only be used in any computer.

5.1.14 Use of unauthorized or pirated software must strictly be prohibited throughout the Bank or NBFI.

5.2 Desktop/Laptop Devices Controls

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

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

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

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

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

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

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

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

5.2.9 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).

5.2.10 Any kind of viruses shall be reported immediately.

5.2.11 Viruses shall not be cleaned/ deleted without expert assistance unless otherwise instructed.

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

5.2.13 Standard virus detection software must be installed on all desktop and laptop computers and shall be configured to check files when read and routinely scan the system for viruses.

5.2.14 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.)

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

5.3 BYOD Controls

"Bring Your Own Device" (BYOD) is a relatively new practice adopted by banks and financial institutions to enable their employees to access corporate email, calendars, applications and data from their personal mobile devices like smart phones, tablet computers, etc. Bank or NBFI shall be aware of the heightened security risks associated with BYOD due to challenges in securing, monitoring and controlling employees' personal devices.

5.3.1 Bank or NBFI shall conduct a comprehensive risk assessment on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.

5.3.2 Bank or NBFI shall not proceed with the BYOD implementation if they are unable to adequately manage the associated security risks.

5.3.3 BYOD is associated with a number of information security risks such as:

a) Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs);
b) Incidents involving threats to, or compromise of, the ICT infrastructure and other information assets (e.g. malware infection or hacking) of Bank or NBFI;
c) Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);
d) Intellectual property rights for information created, stored, processed or communicated on PODs in the course of work for the Bank or NBFI.

Due to information security risks associated with BYOD, employees who wish to opt-in to BYOD must be authorized to do so and must not introduce unacceptable risks onto the banks' networks by failing to secure their own equipment.

5.3.4 The Bank or NBFI may implement appropriate forms of device authentication for PODs approved by authority, such as digital certificates created for each specific device.

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

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

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

5.4 Server Security Controls

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

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

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

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

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

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

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

5.4.8 All unnecessary programs shall be uninstalled from production servers.

5.4.9 In case of virtualization:

a) Bank or NBFI shall plan of setting limit on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM.
b) Host and guest Operating System (OS) must be updated with new/required security patches and other patches if necessary. Patching requirements shall also be applied to the virtualization software.
c) Like physical servers, virtual servers need to be backed up regularly.
d) Bank or NBFI shall ensure that host and guests use synchronized time**.**
e) File sharing shall not be allowed between host and guest OSs, if not required.

5.5 Data Center Controls

As critical systems and data of a Bank or NBFI are concentrated and housed in the Data Center (DC), it is important that the DC is resilient and physically secured from internal and external threats.

5.5.1 Physical Security

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

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

5.5.1.3 Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. The Bank or NBFI shall ensure that visitors are accompanied at all times by an authorized employee while in the DC.

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

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

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

5.5.1.7 Emergency exit door shall be available.

5.5.1.8 Data Center must have a designated custodian or manager in charge to provide authorization and to ensure compliance with Policy.

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

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

5.5.1.11 Where DC is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to bank use must be reviewed and authorized by the Bank or NBFI.

5.5.1.12 The physical security of Data Center premises shall be reviewed at least once each year.

5.5.2 Environmental Security

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

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

5.5.2.3 Development and test environment shall be separated from production.

5.5.2.4 Separate channels for data and power cables to protect from interception or any sort of damages shall be made in the data center.

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

5.5.2.6 Any accessories or devices not associated with Data Center and powered off devices shall not be allowed to store in the Data Center. Separate store room must be in place to keep all sorts of unused and redundant IT equipments.

5.5.2.7 Closed Circuit Television (CCTV) camera shall be installed at appropriate positions of all sides for proper monitoring.

5.5.2.8 The sign of "No eating, drinking or smoking" shall be in display.

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

5.5.2.10 Data Center shall have dedicated telephone communication.

5.5.2.11 Address and telephone or mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT personnel) must be available to meet any emergency necessity.

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

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

5.5.2.14 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) Air conditioners with backup units. Industry standard air conditioning 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

5.5.2.15 The above mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 bases.

5.5.3 Fire Prevention

5.5.3.1 Wall, ceiling and door of Data Center shall be fire-resistant.

5.5.3.2 Fire suppression equipments shall be installed and tested periodically.

5.5.3.3 Automatic fire/smoke alarming system shall be installed and tested periodically.

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

5.5.3.5 Electric cables and data cables in the Data Center must maintain quality and be concealed.

5.5.3.6 Flammable items such as paper, wooden items, plastics, etc. shall not be allowed to store in the Data Center.

5.6 Server/Network Room/Rack Controls

5.6.1 Server/network room/rack must have a glass enclosure with lock and key under a responsible person.

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

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

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

5.6.5 Server/network room/rack shall be air-conditioned. Water leakage precautions and water drainage system from Air Conditioner shall be installed.

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

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

5.6.8 Proper attention must be given on overloading electrical outlets with too many devices.

5.6.9 Channel alongside the wall shall be prepared to allow all required cabling in neat and safe position as per layout of power supply and data cables.

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

5.6.11 Power supply shall be switched off before leaving the server room if otherwise not required.

5.6.12 Fire extinguisher shall be placed outdoor visible area of the server room. This must be maintained and checked on an annual basis.

5.7 Networks Security Management

5.7.1 The Bank or NBFI shall establish baseline standards to ensure security for Operating Systems, Databases, Network equipments and portable devices which shall meet organization's policy.

5.7.2 The Bank or NBFI shall conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

5.7.3 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.

5.7.4 All type of cables including UTP, fiber, power shall have proper labeling for further corrective or preventive maintenance works.

5.7.5 The Bank or NBFI shall ensure physical security of all network equipments.

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

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

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

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

5.7.10 Secure Login feature (i.e. SSH) shall be enabled in network devices for remote administration purposes. Any unencrypted login option (i.e. TELNET) shall be disabled.

5.7.11 The Bank or NBFI shall backup and review rules on network security devices on a regular basis to determine that such rules are appropriate and relevant.

5.7.12 The Bank or NBFI shall establish redundant communication links for WAN connectivity.

5.7.13 The Bank or NBFI deploying Wireless Local Area Networks (WLAN) within the organization shall be aware of risks associated in this environment. Secure communication protocols for transmissions between access points and wireless clients shall be implemented to secure the corporate network from unauthorized access.

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

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

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

5.7.17 Real time health monitoring system for infrastructure management may be implemented for surveillance of all network equipments and servers.

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

5.7.19 The Bank or NBFI shall change all default passwords of network devices.

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

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

5.7.22 Role-based administration shall be ensured for the servers.

5.8 Cryptography

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

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

5.8.1 The Bank or NBFI shall establish cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation and expiry.

5.8.2 The Bank or NBFI shall ensure that cryptographic keys are securely generated. All materials used in the generation process shall be destroyed after usage and ensure that no single individual knows any key in its entirety or has access to all the constituents making up these keys.

5.8.3 Cryptographic keys shall be used for a single purpose to reduce the impact of an exposure of a key.

5.8.4 The effective timeframe that a cryptographic key may be used in a given cryptographic solution is called the cryptoperiod. The Bank or NBFI shall define the appropriate cryptoperiod for each cryptographic key considering sensitivity of data and operational criticality.

5.8.5 The Bank or NBFI shall ensure that hardware security modules and keying materials are physically and logically protected.

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

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

5.8.8 In the event of changing a cryptographic key, the Bank or NBFI shall generate the new key independently from the previous key.

5.8.9 The Bank or NBFI shall maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys shall be accorded to backup keys.

5.8.10 If a key is compromised, the Bank or NBFI shall immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. The Bank or NBFI shall inform all parties concerned of the revocation of the compromised keys.

5.9 Malicious Code Protection

5.9.1 The environment of Banks or NBFIs including servers and workstations must be protected from malicious code by ensuring that approved anti-virus packages are installed.

5.9.2 Users must be made aware of arrangements to prevent and detect the introduction of malicious software.

5.9.3 Software and data supporting critical business activities must be regularly scanned or searched to identify possible malicious code.

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

5.9.5 Attachments to electronic mail must be checked for malicious code before use.

5.9.6 The anti-virus package must be kept up to date with the latest virus definition file using an automated and timely process.

5.9.7 All computers in the network shall get updated signature of anti-virus software automatically from the server.

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

5.9.9 A computer virus hoax is a message warning the recipients of a non-existent computer virus. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know. Employees must be made aware of the problem of hoax viruses and must not forward such virus alarms.

5.9.10 A formal process for managing attacks from malicious code must include procedures for reporting attacks and recovering from attacks.

5.9.11 Bank or NBFI may arrange awareness program for the end users about computer viruses and their prevention mechanism.

5.10 Internet Access Management

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

5.10.2 Access to and use of the internet from bank premises must be secure and must not compromise information security of Bank or NBFI.

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

5.10.4 Any local connection directly to the Internet from Bank or NBFI premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security.

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

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

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

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

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

5.11 Email Management

5.11.1 Email system shall be used according to the Bank's or NBFI's policy.

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

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

5.11.4 Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.

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

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

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

5.11.8 Email transmissions from the Bank or NBFI must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

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

5.12 Vulnerability Assessment and Penetration Testing

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

5.12.1 The Bank or NBFI shall conduct VAs regularly to detect security vulnerabilities in the ICT environment.

5.12.2 The Bank or NBFI shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA shall include common web vulnerabilities such as SQL injection, cross-site scripting, etc.

5.12.3 The Bank or NBFI shall establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

5.12.4 The Bank or NBFI shall carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of

actual attacks on the system. The Bank or NBFI shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

5.13 Patch Management

5.13.1 The Bank or NBFI shall establish and ensure that the patch management procedures include identification, categorization and prioritization of security patches. To implement security patches in a timely manner, the Bank or NBFI shall establish the implementation timeframe for each category of security patches.

5.13.2 The Bank or NBFI shall perform rigorous testing of security patches before deployment into the production environment.

5.14 Security Monitoring

5.14.1 The Bank or NBFI shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.

5.14.2 The Bank or NBFI shall implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the Bank or NBFI against network intrusion attacks as well as provide alerts when an intrusion occurs.

5.14.3 The Bank or NBFI may implement security monitoring tools which enable the detection of changes to critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes.

5.14.4 The Bank or NBFI shall regularly review security logs of systems, applications and network devices for anomalies. Logs shall be protected and retained for defined period to facilitate future investigation.

Chapter 6

6. Access Control of Information System

The Bank or NBFI shall only grant access rights and system privileges based on job responsibility. The Bank or NBFI shall check that no person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities for legitimate purposes.

6.1 User Access Management

6.1.1 The Bank or NBFI shall only grant user access to ICT systems and networks on a need-to-use basis and within the period when the access is required.

6.1.2 The Bank or NBFI shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions.

6.1.3 Each user must have a unique User ID and a valid password.

6.1.4 User ID Maintenance form with access privileges shall be duly approved by the appropriate authority.

6.1.5 User access shall be locked for unsuccessful login attempts.

6.1.6 User access privileges must be kept updated for job status changes.

6.1.7 The Bank or NBFI shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

6.1.8 The Bank or NBFI shall perform regular reviews of user access privileges to verify that privileges are granted appropriately.

6.2 Password Management

6.2.1 The Bank or NBFI shall enforce strong password controls over users' access.

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

6.2.3 Password definition parameters shall ensure that minimum password length is maintained according to Bank's Policy (at least 6 characters).

6.2.4 Password shall be combination of at least three of stated criteria like uppercase, lowercase, special characters and numbers.

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

6.2.6 Parameter to control maximum number of invalid logon attempts shall be specified properly in the system according to the Bank's Policy (maximum 3 consecutive times).

6.2.7 Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least three (3) times.

6.2.8 Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope.

6.3 Input Control

6.3.1 Session time-out period for users shall be set in accordance with the Bank's Policy.

6.3.2 Operating time schedule of users' input for banking applications shall be implemented as per regulatory enforcement unless otherwise permitted from appropriate authority.

6.3.3 Audit trail with User ID and date-time stamp shall be maintained for data insertion, deletion and modification.

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

6.3.5 Management approval must be in place for delegation of authority.

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

6.4 Privileged Access Management

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

6.4.1 The Bank or NBFI shall apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.

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

a) Implement strong authentication mechanisms;
b) Implement strong controls over remote access;
c) Restrict the number of privileged users;
d) Grant privileged access on a "need-to-have" basis;
e) Review privileged users' activities on a timely basis;
f) Prohibit sharing of privileged accounts;

g) Disallow vendors from gaining privileged access to systems without close supervision and monitoring;

Chapter 7

7. Business Continuity and Disaster Recovery Management

Business Continuity and Disaster Recovery Management is required for planning of business resiliency for critical incidents, operational risks take into account for wide area disasters, Data Center disasters and the recovery plan. The primary objective of Business Continuity Plan (BCP) is to enable a Bank or NBFI to survive in a disaster and to re-establish normal business operations. In order to survive with minimum financial and reputational loss, Bank or NBFI shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning. Contingency plan shall also address the backup, recovery and restore process.

7.1 Business Continuity Plan (BCP)

7.1.1 Bank or NBFI must have an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.

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

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

7.1.4 The BCP shall be coordinated with and supported by the Business Impact Analysis (BIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.

7.1.5 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, venders and agencies.
c) Grab list of items such as backup tapes, laptops, flash drives, etc.
d) Disaster recovery site map

7.1.6 BCP must be tested and reviewed at least once a year to ensure the effectiveness.

7.2 Disaster Recovery Plan (DRP)

7.2.1 Bank or NBFI must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the Bank or NBFI shall include a scenario analysis to identify and address various types of contingency scenarios. The Bank or NBFI shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.

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

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

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

7.2.5 Physical and environmental security of the DRS and/or Near DC shall be maintained.

7.2.6 The Bank or NBFI shall define system recovery and business resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.

7.2.7 The Bank or NBFI shall consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.

7.2.8 The Bank or NBFI may explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the bank's recovery capability.

7.2.9 Information security shall be maintained properly throughout the recovery process.

7.2.10 An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.

7.2.11 The Bank or NBFI shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

7.2.12 The Bank or NBFI shall involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly.

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

7.3 Data Backup and Restore Management

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

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

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

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

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

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

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

7.3.8 At least one copy of backup shall be kept on-site for the time critical delivery.

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

7.3.10 The Bank or NBFI shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the bank’s recovery process.

Chapter 8

8. Acquisition and Development of Information Systems

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

Many systems fail because of poor system design and implementation, as well as inadequate testing. The Bank or NBFI shall identify system deficiencies and defects at the system design, development and testing phases. The Bank or NBFI shall establish a steering committee, consisting of business owners, the development/technical team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realized at each phase of the project and milestones to be reached according to the project timetable.

8.1 ICT Project Management

8.1.1 In drawing up a project management framework, the Bank or NBFI 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, definition of project milestones and deliverables. The Bank or NBFI shall clearly define in the project management framework, the roles and responsibilities of staff involved in the project.

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

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

8.1.4 The Bank or NBFI shall establish management oversight of the project to ensure that milestones are reached and deliverables are realized in a timely manner.

8.2 Vendor Selection for System Acquisition

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

8.2.2 Vendor selection process must have conformity with the Procurement Policy of the Bank or NBFI.

8.2.3 Vendor selection criteria for application must address followings:

a) Market presence
b) Years in operation
c) Technology alliances
d) Extent of customization and work around solutions
e) Financial strength
f) Performance and Scalability
g) Number of installations
h) Existing customer reference
i) Support arrangement
j) Local support arrangement for foreign vendors
k) Weight of financial and technical proposal

8.3 In-house Software Development

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

8.3.2 Detailed technical requirements and design shall be prepared.

8.3.3 Application security and availability requirements shall be addressed.

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

8.3.5 Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.

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

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

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

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

8.3.10 Application shall be in compliance with relevant controls of Bank's ICT Security Policy.

8.3.11 Necessary '*Regulatory Compliance*' requirements must be taken into account by the Bank or NBFI.

8.4 Software Documentation

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

8.4.2 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

8.5 Statutory Requirements

8.5.1 All the software procured and installed by the Bank or NBFI shall have legal licenses and record of the same shall be maintained by the respective unit/department of the Bank or NBFI.

8.5.2 There shall have a separate test environment to perform end-to-end testing of the software functionalities before implementation.

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

8.5.4 Necessary Regulatory Compliance requirements for banking procedures and practices and relevant laws of Government of Bangladesh must be taken into account.

8.5.5 Any bugs and/or defects found due to design flaws must be escalated to higher levels in Software Vendors' organization and Bank/NBFI in time.

8.5.6 Support agreement must be maintained with the provider for the application software used in production with the confidentiality agreement.

Chapter 9

9. Alternative Delivery Channels (ADC) Security Management

"Channelize through channels" is the new paradigm for banking today, which in earlier relied solely on the branch network. Branchless banking is a distribution channel strategy used for delivering financial services without relying on bank branches. Alternate Delivery Channels are methods for providing banking services directly to the customers. Customers can perform banking transactions through their ATM, contact the bank's Call Center for any inquiry, access the digital Interactive Voice Response (IVR), perform transactions through Internet Banking and even on phones through mobile banking, etc. These channels have enabled banks to reach a wide consumer-base regardless of time and geographic location. ADCs ensure higher customer satisfaction at lower operational expenses and transaction costs.

9.1 ATM/POS Transactions

The ATMs and Point-of-Sale (POS) devices have facilitated cardholders with the convenience of withdrawing cash as well as making payments to merchants and billing organizations. However, these systems are targets where card skimming attacks are perpetrated. To secure consumer confidence in using these systems, the Bank or NBFI shall consider putting in place the following measures to counteract fraudsters' attacks on ATMs and POS devices:

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

9.1.2 The Bank or NBFI shall install detection mechanisms and send alerts to appropriate staff for follow-up response and action.

9.1.3 The Bank or NBFI shall implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission.

9.1.4 The Bank or NBFI shall implement appropriate measures to prevent shoulder surfing of customers' PINs.

9.1.5 The Bank or NBFI may implement biometric finger vein sensing technology to resist PIN compromise.

9.1.6 The Bank or NBFI shall conduct video surveillance of activities for 24 hours at these machines and maintain the quality of CCTV footage and preserve for at least one year.

9.1.7 The Bank or NBFI shall introduce a centralized online monitoring system for Cash Balance, Loading-Unloading functions, Disorders of machine, etc.

9.1.8 The Bank or NBFI shall deploy security personnel for all ATM devices 24 hour basis.

9.1.9 The Bank or NBFI shall verify that adequate physical security measures are implemented in ATM devices.

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

9.1.11 Bank or NBFI shall monitor third party cash replenishment vendors' activities constantly and visit third party cash sorting houses regularly.

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

9.1.13 The Bank or NBFI shall educate its customers on security measures that are put in place by the Bank or NBFI and are to maintain by the customers for ATM and POS transactions.

9.2 Internet Banking

Information involved in internet banking facility passing over public networks shall be protected from fraudulent activity, dispute and unauthorized disclosure or modification. Banks' internet systems may be vulnerable as financial services are increasingly being provided via the internet. As a counter-measure, the Bank or NBFI shall devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

9.2.1 The Bank or NBFI shall provide assurance to its customers and users so that online access and transactions performed over the internet are adequately protected and authenticated.

9.2.2 Bank or NBFI shall properly evaluate security requirements associated with its internet banking system and adopt mechanisms which are well-established international standards.

9.2.3 The Bank or NBFI shall formulate Internet Banking Security policy considering technology security aspects as well as operational issues.

9.2.4 The Bank or NBFI shall ensure that information processed, stored or transmitted between the bank and its customers is accurate, reliable and complete. The Bank

or NBFI shall also implement appropriate processing and transmission controls to protect the integrity of systems and data, e.g. SSL, TLS.

9.2.5 The bank shall implement 2-FA (two-factor authentication) for all types of online financial transactions. Hardware/Software based tokenization means will be preferred. The primary objectives of two-factor authentication are to secure the customer authentication process and to protect the integrity of customer account data and transaction details as well as to enhance confidence in online systems.

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

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

9.2.8 All system accesses, including messages received shall be logged. Security violations (suspected or attempted) shall be reported and followed up. Bank may acquire tools for monitoring systems and networks against intrusions and attacks.

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

9.2.10 The Bank or NBFI shall take appropriate measures to minimize exposure to other forms of attacks such as middleman attack which is commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

9.2.11 The information security officer or any other assigned person/team shall undertake periodic penetration tests of the system, which may include:

a) Attempting to guess passwords using password-cracking tools
b) Searching for back door traps in the programs
c) Attempting to overload the system using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks
d) Checking middleman attacks
e) Checking of commonly known holes in the software, especially the browser and the e-mail software exist
f) Checking the weaknesses of the infrastructure

g) Taking control of ports
h) Cause application crash
i) Injecting malicious codes to application and database servers

9.2.12 The Bank or NBFI shall educate its customers on security measures to protect them in an online environment.

9.3 Payment Cards

Payment cards allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase over the internet, through mail-order or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines ("ATMs").

Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including ATMs, payment kiosks and POS terminals.

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

9.3.2 The Bank or NBFI shall ensure that the processing of sensitive or confidential information is done in a secure environment.

9.3.3 The Bank or NBFI shall deploy secure chips with multiple payment application supported to store sensitive payment card data. For interoperability reasons, where transactions could only be resulted by using information from the magnetic stripe on a card, the Bank or NBFI shall ensure that adequate controls are implemented to manage these transactions.

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

9.3.5 Equipments used to generate payment card PINs and keys shall be managed in a secured manner.

9.3.6 Card personalization, PIN generation, Card distribution, PIN distribution, Card activation groups shall be different from each other.

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

9.3.8 The Bank or NBFI shall only activate new payment cards upon obtaining the customer's instruction.

9.3.9 The Bank or NBFI shall implement a dynamic one-time-password ("OTP") as 2-FA for CNP (Card Not Present) transactions via internet to reduce fraud risk associated with it.

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

9.3.11 The Bank or NBFI 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.

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

9.4 Mobile Financial Services

Controls over mobile transactions are required to manage the risks of working in an unprotected environment. The Bank or NBFI shall formulate security controls, system availability and recovery capabilities, which commensurate with the level of risk exposure, for operations.

9.4.1 Security standards shall be followed appropriate to the complexity of services offered.

9.4.2 Banks or NBFIs shall clearly identify risks associated with the types of services being offered in the risk management process.

9.4.3 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.

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

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

9.4.6 Bank or NBFI shall conduct periodic risk management analysis and security assessment of the MFS operation and take appropriate measures accordingly.

9.4.7 Bank or NBFI shall have conformity with '*Regulatory Compliance'* requirements of the country.

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

Chapter 10

10. Service Provider Management

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

10.1 Outsourcing

Now-a-days commercial banks outsource their different ICT services. Agreements of such outsourcing arrangement usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

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

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

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

a) Objective behind Outsourcing
b) Economic viability
c) Risks and security concerns.

10.1.4 ICT outsourcing shall not result in any weakening or degradation of the bank's internal controls. The Bank or NBFI shall require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, object programs and source codes.

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

10.1.6 The Bank or NBFI shall monitor and review the security policies, procedures and controls of the service provider on a regular basis, including periodic expert

reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

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

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

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

10.2 Cross-border System Support

10.2.1 The Bank or NBFI 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.

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

10.3 Service Level Agreement

10.3.1 There shall have Service Level Agreements between the Bank or NBFI and vendors.

10.3.2 The Annual Maintenance Contract (AMC) with the vendor shall be active and currently in-force.

10.3.3 Dashboard with significant details for SLAs and AMCs shall be prepared and kept updated.

10.3.4 Bank or NBFI shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

10.3.5 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.

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

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

Chapter 11

11. Customer Education

With the advent of electronic banking, customer's experience of banking is therefore no longer fully under control of a Bank or NBFI. In the age of self-service banking model, a customer also has to be equipped to do safe banking through self help. It is often said that the best defense against frauds is awareness of customer. With fraudsters constantly creating more diverse and complex fraudulent ruses using advanced technology and social engineering techniques to access their victims' accounts, accelerating awareness among consumers becomes imperative.

It is also important to educate other stakeholders, including bank employees, who can then act as resource persons for customer queries, law enforcement personnel for more understanding response to customer complaints and media for dissemination of accurate and timely information.

11.1 Awareness Program

Awareness programs can be successful only if users feel the content is in their interest and is relevant to their banking needs. For fruitful awareness program to be arranged, the bank needs to identify personnel, awareness material, advertisements and promotions and maintenance of website.

11.1.1 The needs of the target audience shall be identified, appropriate budgets obtained and priorities established.

11.1.2 The work plan shall clearly mention the main activities with the required resources, timelines and milestones.

11.1.3 The Bank or NBFI shall create and publish proper contents.

11.1.4 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 to identify areas vulnerable to fraud attempts and make them aware of their responsibilities in relation to fraud prevention.
c) Motivate individuals to adopt recommended guidelines or practices.
d) Create a stronger culture of security with better understanding and commitment.
e) Help minimize the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly (reduced need to investigate).

11.1.5 The Bank or NBFI shall deliver the right message content to the right audience using the most effective communication channels.

11.1.6 Awareness building collaterals can be created in the form of:

a) Leaflets and brochures
b) Short Messaging Service (SMS) texts
c) Safety tips in account statements and envelopes
d) Educational material in account opening kits
e) Receipts dispensed by ATM/POS
f) Screensavers
g) Electronic newsletters
h) DVDs with animated case studies and videos
i) Recorded messages played during waiting period of phone banking calls

11.1.7 Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.

a) Advertising campaigns though print and TV media
b) ATM screens , Emails and SMS texts
c) Common website developed with content from all stakeholders
d) Groups, games and profiles on social media
e) Advertisements on online shopping sites
f) Bill boards
g) Online training modules and demos hosted on this site
h) Posters in prominent locations such as petrol pumps, popular restaurants, shopping malls, etc.
i) Interactive guidance in the form of helplines
j) Customer meets and interactive sessions with specialists
k) Talk shows on television/radio

11.1.8 Continuous improvement cannot occur without knowing how the existing program is working. A well-calibrated feedback strategy must be designed and implemented.

Glossary and Acronyms

2FA	- Two-Factor Authentication
ADC	- Alternative Delivery Channel
AMC	- Annual Maintenance Contract
AML	- Anti-Money Laundering
ATM	- Automated Teller Machine
BCP	- Business Continuity Plan
BIA	- Business Impact Analysis
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
CISO	- Chief Information Security Officer
CNP	- Card Not Present
CTO	- Chief Technology Offier
DC	- Data Center
DDoS	- Distributed Denial of Service
DoS	- Denial of Service
DR	- Disaster Recovery
DRP	- Disaster Recovery Plan
DRS	- Disaster Recovery Site
DVD	- Digital Video Disc
E-mail	- Electronic Mail
EOD	- End of Day
ICC	- Internal Control and Compliance
ICT	- Information and Communication Technology
IDS	- Intrusion Detection System
IPS	- Intrusion Prevention System
IS	- Information System
ISDN	- Integrated Services Digital Network
ICT	- Information and Communication Technology
IVR	- Interactive Voice Response
JD	- Job Description
KRIs	- Key Risk Indicators
MITMA	- Man-in-the-Middle Attack
NBFI	- Non-Bank Financial Institution
OTP	- One Time Password

PCI DSS	- Payment Card Industry Data Security Standard
PCs	- Personal Computers
PDA	- Personal Digital Assistant
PIN	- Personal Identification Number
PODs	- Personally Owned Devices
POS	- Point of Sale
PSTN	- Public Switched Telephone Network
RPO	- Recovery Point Objective
RTO	- Recovery Time Objective
SDLC	- Software Development Life Cycle
SMS	- Short Messaging Service
SQL	- Structured Query Language
SSL	- Secured Socket Layer
TV	- Television
UAT	- User Acceptance Test
UPS	- Uninterrupted Power Supply
USB	- Universal Serial Bus
User ID	- User Identification
UTP	- Unshielded Twisted Pair
VA	- Vulnerability assessment
VLAN	- Virtual Local Area Network
VPN	- Virtual Private Network
WAN	- Wide Area Network
WLAN	- Wireless Local Area Network