Bangladesh Commerce Bank Limited

IT Security Policy

Version 4.0

IT Division, Head Office
October 2016

Table of Contents

Annexure:

Chapter -1

1. Introduction

Information and communication technology systems are essential assets of the banks and as well as for their customers and stakeholders. Moreover, security of IT systems for a financial institution has therefore gained much greater in importance, and it is vital that we ensure such risks are properly identified and managed. In this circumstance, we should design/ maintain the system efficiently and should take necessary steps to protect the information from unauthorized access, modification, disclosure and destruction.

BCBL is committed to ensuring the privacy of the Divisions, its employees, and its partners from unauthorized, illegal, and malicious actions by individuals, intentionally or otherwise.

The purpose of the BCBL IT Policy is to give clear guidelines, rules & regulation for all activities and operations related to data security, facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other intellectual property rights to protect the Bank and its employees.

1.1 Scope

This policy applies to all BCBL employees, both permanent and temporary, within the bank, including the employees of the Bank's service partners. This policy applies to all equipment that is owned, leased, operated, or maintained by the Bank. This policy also applies to any equipment connected to the BCBL LAN or WAN.

1.2 Objectives

The objective of this document is to lay out the security standard for all Information Technology (IT) equipment that will protect the Trust, its patients / clients, members of staff and ensure that all BCBL executive guidelines are met.

- Shall ensure that all current and future staff is instructed in their information security responsibilities.
- Shall ensure that all their staff using computer systems/media are trained in their use.
- Shall ensure that no unauthorized staff are allowed to access any of the Bank's computer systems as such access could compromise data integrity
- Shall determine which individuals are to be given authority to access specific computer systems. The level of access to all systems, buildings and offices shall be based on job function need, independent of status
- Shall ensure that current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability
- Has legal obligations to maintain security and confidentiality IT SECURITY POLICY

1.3 Categorization of banks/branches/units depending on IT Operation

The locations for which the IT Guideline is applicable i.e., the Head Office, Branch and Booth of a bank may be categorize into three tiers as under depending on their IT setup and operational environment / procedures:

Tier-1: Centralized IT Operation of Data Center (DC) including Disaster Recovery Site (DRS) to which all other offices, branches and booths are connected through WAN with 365x7x24 hours attended operation.

Tier-2: Head Office, Branch or booth having Server to which all or a part of the computers of that locations are connected through LAN.

Tier-3: Head Office, Branch or booth having stand-alone computer(s), Laptop(s), ATM(s) or Mobile devices.

The proposed ICT Policy will be applicable for all the three tiers if not mentioned otherwise.

Chapter -2

2 IT Security Management:

IT Security Management must ensure that the IT functions and operations are efficiently and effectively managed. Head of IT will supervise team leaders of three groups in addition of his following responsibilities.

Head of IT:

1. Overall Management of the IT division
2. Liaison with different divisional Heads & Branch managers to identify the risks associated with IT related products and their expectations from IT division.
3. Supervise software, network, communication and hardware operation & their maintenance.
4. Responsible for providing IT solutions to meet business objectives
5. Liaison with 3rd party Vendors to finalize the deal of purchase and maintenance/service level agreements
6. Monitoring of security, implemented policies & practices.
7. Development of various policies and their implementation in divisions and branches.
8. Supervise Branch opening issues and new projects
9. Compliance of issues raised by external or internal IT Auditor.
10. Resource allocation and task assignment.
11. Testing of disaster recovery & business continuity plan.
12. Strategic planning for development, training & upgradation.
13. Development of various MIS reports to aid for decision-making process for management.

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 and ICT Security Unit

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 IT Security Policy

- Ensuring that all staff under their control are aware and comply with the IT Security Policy
- Ensuring that staff have the necessary access level appropriate to their role within the BCBL
- Ensuring that when a member of staff's role changes, any amendments to the access level required are requested in writing (using the Request for Change Process) to the IT Division.
- Ensuring that when a staff member leaves BCBL, including temporary staff or contractors, the IT division is contacted immediately
- Ensuring that all staff within the BCBL complies with the current laws relating to information security &management.
- Ensuring that computer systems are used as they were intended
- Reporting any breaches of the IT Security Policy to the Head of IT.
- Ensure that all portable devices such as laptops and mobile phones are recovered when staff leave or move within the branches / divisions. Confirmation of this must be sent to the IT division and devices returned for cleansing and redeployment

2.3 Documentation :

Organogram Chart:

The organogram chart of IT Division is given in Annexure - 5.

Job Description & segregation of duties:

The operation & activities of IT Division are segregated and assigned in three major groups –i) Software Operations, Development & Implementation, ii) Communications, Network & Hardware and iii) Project Implementation.

Similarly, the IT personnel are divided into three groups to accomplish all related tasks although there is a provision to transfer internally whenever required or suggested by senior management. Although duties of each group members are segregated to balance the workload, all of them are wholly responsible for tasks assigned to each group.

Software Operation, Development & Implementation: This group is solely responsible for smooth operation, troubleshooting, maintenance and new development & implementation of core banking

software or other installed software (licensed, rented or purchased) at Data center, all branches and divisions of BCBL. They are equally responsible for the software developed BCBL, Bangladesh Bank or third party/ vendors.

1. Provide development, troubleshooting & support for existing automated system.
2. Administration and maintenance of all implemented System. Team leader of the group will act as Data Base Administrator (DBA).
3. Planning & providing MIS reports as per requirement from system
4. Comply with the new requirements and enhancement of existing software solutions.
5. Analyze & Investigate software requirement for the bank & its Division
6. Design and development of new software system solution
7. Testing and evaluation of new system according to business rule for in-house or vendor supplied. Testing of new software/ banking S/W modules with different parameter before deployment.
8. Implementation and maintenance of new system/ modules
9. Preparation and delivery of user and administration documents for operation of in-house developed S/W
10. Training and Development of IT personnel & end users of all Branches and Head office level.
11. Managing the current process that complies with the requirements
12. Ensuring regular System Backup (Tape, DVD and HDD), Disaster recovery maintenance both at Branch and Head office level as per policy
13. Ensuring proper accounting, creation of GL head and maintaining unique Chart of Accounts, user limits, rights & privileges as per Banks' circular at all branches and head office.
14. Suggestion for improvements in all systems and make interaction with branch users/operators in these regards.
15. Installation / up gradation of third party installed software or regulatory developed software.
16. Planning & changing of policies whenever required.
17. Any other work allocated by the divisional Head.

Communication, Network & Hardware: This group is solely responsible for the smoother operation, troubleshooting, maintenance of all communication & network devices, connectivity and servers, workstations & other peripherals (leased, rented or purchased) at Data center, all branches and Division of BCBL.

1. Design, development & analysis of Communications & Network infrastructure
2. Management of LAN/WAN equipment such as Routers, Switches, HUB etc. to ensure smooth operation.
3. Supervising of internet, intranet connectivity issues and bandwidth & traffic management.
4. Implementation & monitoring policy and ensuring network device security.
5. Maintenance of security for Firewall & Network and documentation of configuration of all installation
6. Installation and upgradation of Antivirus for corporate HO and branches.
7. Installation, maintenance and recovery of Email server, proxy server.
8. Backup/Restore of all servers such as Email, proxy, firewall etc.
9. Ensuring Business Continuity for all Branches and Divisions.
10. Diagnosis of Printer, UPS and monitor failure and if necessary, communicate with vendor for spares.

11. Liaison with 3rd party Vendors with regards to maintenance & contracts. Preparation of SLA or renewal of SLA related to all parties
12. Requirement analysis for purchase of hardware and other equipment.
13. Inviting quotation and make comparative & cost benefit analysis for requirements.
14. Installation of workstations, printers, scanner and other peripherals for existing or newly opened branches.
15. Installation of OS, service packs, other patches and related software utilities required for smooth operation.
16. Analyzing the repetition of faults / errors reported by branches to prevent future occurrence of same issues in case of hardware, network or communication devices.
17. Planning & changing of policies whenever required.
18. Any other work allocated by the Divisional Head.

Project Implementation: This group is solely responsible planning, implementation & successful operation of all projects would be taken by Bank under the umbrella of Information technology dept. These could be related software, communications, network or hardware.

1. Feasibility study of the project assigned by senior management, which could be related to software, communications, network or hardware.
2. Site visit, strategic planning & liaison with related parties and vendors.
3. Preparation of documentation related to planning, implementation & costing.
4. Leading and organizing personnel and logistic support to finish the project as per schedule.
5. Supervising closely at the time of implementation and report to senior management about the progress of project.
6. Conducting test run and monitoring of all activities at the time of LIVE operation and reporting to senior management about the variance of expectation and real operation.
7. Change of Planning & policies whenever required after taking approval from senior management.
8. Any other work allocated by the division Head.

Fallback Plan: IT Personnel: Regarding fallback plan of IT personnel, we have divided all IT activities into three categories and recruited required IT professionals in each area of concentration to avoid possible hazards in case of resignation/ long vacation. This is equally applicable for IT support personnel and senior management of IT Division. The name & designation of the IT personnel in each group were mentioned in organogram chart (Annexure-I), which may be reviewed/ changed whenever required (at least once in a year). The fallback plan of IT personnel was and should be tested by letting at least one of the members from each group for a long vacation or outside training and assigning ones tasks to another to find out whether the plan will work satisfactorily or not. If discrepancy arises in future, necessary changing and job orientation will be done immediately.

Datacenter: Datacenter fallback plan is incorporated later in the part of Business Continuity & Disaster Recovery Plan.

Branch: Disaster Recovery & Business Continuity Plan for branch is detailed later in the above mentioned part.

2.4 Internal Information System Audit:

The Bank is required to ensure regulatory compliance at all levels; therefore, IT Audit is aimed at ensuring an acceptable standard for security on all BCBL servers, workstations, routers, switches, and other IT systems. Additionally, it should ensure that proper purchase and approval procedure are followed, the documentation are correct and the inventory reflects accurate IT Asset value. The IT Audit policy is developed to comply with the findings of the IT Audit Cell of the Central Bank (Bangladesh Bank) which is detailed below.

a. Check documentary compliance, record-keeping and conformance to approval process and inventory:

i) To ensure proper approval procedure is followed for purchase
ii) To ensure payment disbursed reflects correct approval amounts and specifications
iii) To ensure approved purchases and invoices reflect correctly upon current Inventory of IT equipments
iv) To ensure fair conduct and treatment in obtaining quotations and tender bids
v) To ensure IT equipment and specifications reflect fair pricing in quotations and purchase
vi) To ensure satisfactory certificate is obtained from the user when a new system is delivered/installed or when the existing system is repaired or replaced
vii) To ensure correct record keeping and acquiescence to gate-pass issuance for IT equipment sent outside of the Bank's premises for repair/replacement
viii) To ensure compliance to Bank's write-off procedure for all IT Assets in case of equipment being not repairable or have fully depreciated
ix) Other elements may be added as and when required

b. Conduct IT System security Audit for the following reasons:

i) To ensure integrity, confidentiality and availability of information and resources
ii) To investigate possible security vulnerabilities and incidents in order to ensure conformance to the Bank's security policies
iii) To ensure software systems deployed conforms to the Bank's software implementation policy
iv) To ensure changes made to any systems conforms to the Bank's Change Control/Change Management policy. In this connection, a report will be available consisting a) table name, b) existing value, c) changed value, d) user id, e) date-time.
v) To ensure regular Backup of data and business critical system is taken
vi) To ensure Restore of both data and full system is carried out on a regular basis, so that data integrity can be ensured and the Bank can be prepared for any possible disaster
vii) To monitor user or system activity where appropriate
viii) Upon request

c. When requested, and for the purpose of performing IT Audit, any access needed will be provided to the IT Audit Specialist/Team. This access may include:

i) Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on the Bank's equipment or premises
ii) Access to work areas (Server Rooms, office desks, cubicles, storage areas etc.)
iii) Access to interactively monitor and log traffic on the Bank's corporate network in conjunction with Bank's WAN connectivity provider

iv) Moving machines involved in an incident to a safe location for analysis or to ensure evidence is captured and preserved securely
v) User level and/or Admin level access to any computing or communications devices
vi) Access required to perform network or host scans and obtain any applicable information

d. IT Audit may be conducted by any member of the IT System Audit Team/Internal Control and Compliance Division as authorized by the competent authority of the Bank. These member(s) will, on request, produce identification identifying them as members of Bank's IT System Audit Team/Internal Control and Compliance Division. The three phases of the audit process are:

Pre-Audit:

1. All Audits shall be conducted by appointment/surprise
2. For Audits made by appointment an audit checklist may be made available prior to the audit.

Audit: consists primarily of

i) Personnel interviews
ii) Files and documentations check
iii) Counts of IT equipment (Inventory)
iv) Server & workstations check
v) Network scans
vi) Vulnerability scanning

Post Audit:

i) Each audit will result in a follow-up report possibly including an action plan, which will be presented to the IT In-Charge, the owner of responsibility, and the Senior Management. For audits carried out at the branches, a copy of the above mentioned report may be provided to the Branch In-Charge
ii) The IT In-Charge or owner must outline an acceptable remediation plan with the Auditor within 0-5 business days, depending on the criticality of the action items
iii) Remediation: The IT In-Charge and Owner of the Responsibility are responsible for taking appropriate action to complete the tasks on the remediation plan within the agreed-upon deadlines
iv) Remediation: It is the responsibility of the officer/administrator to perform proper contingency steps and conformance to Change Management Policy prior to making these changes (backup, recording of parameters and settings etc.). Once, the changes are applied ensure proper tests are carried out on the system and adequate logs are maintained

e**.** The owner of the responsibility/ Branch in-Charge or a delegate of the applicable IT Division must be present whenever IT Audit is conducted

f. In the event of a system compromise involving a machine that maintains sensitive data or information, the IT Audit Specialist/Team must sign-off on the remediation and re-audit the machine before it is put back into the production environment.

g. The IT Audit Specialist/Team will not be responsible for performance degradation/availability of the system which may be affected by network or host scanning unless the damage is caused by gross negligence or misconduct. We have groomed up couple of IT personnel to perform IT & Communication Security Audit at all branches and various Division. A checklist & plan were provided to them for IT audit

reporting & compliance. It may be noted here that internal IT audit for branches & Divisions should be performed at least once in a year.

2.5 External Information System Audit

2.5.1 Bank 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 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 Training and Awareness:

Training is a continuous process for each employee to become expert in related fields. Basic banking training is given to all of our IT personnel. Moreover, they are being trained in the areas of communication, network (CCNA) and database (OCP) to increase the command in the area of specialization. To keep updated with the changing environment, they will be sent for more outside training in near future. We have completed couple of in-house training to all officers who came from various branches and division. These are being conducted in the light of IT Operations, security issues & core banking solutions. In this connection, user manuals & training materials have been prepared for distribution. More training programs are being planned for Officers & Executives of branches & various division related to security, importance & awareness of IT activities, virus infection/ remedy and illegal or unauthorized access. We shall also be including Branch IT Admin officers who will be trained to work as a representative of IT division in addition to his/her regular assignment.

2.8 Insurance or Risk Coverage Fund:

Most of the IT assets are leased properties which are under insurance coverage of fire only. We are in the process of getting approval for insurance for all assets from natural disaster (flood, earthquake and other natural calamities.) & burglar. Moreover, we are still searching for an insurance company who will facilitate us data insurance.

2.9 Problem Management:

We have created a help desk/ support center where all IT related problems are routed. If problems are related to operational/ data errors, these are being responded immediately. If problems are stemmed from banking system/ hardware, these are being segregated for research & development. In this connection, log sheets are being maintained to entry, assign and record status of problems reported from all branches & division. These logs are being reviewed by Head of IT once in a month. System/ hardware related problems are documented & sent for designated IT personnel for investigation. ISO forms are being used. After rectification/modifications, methods/steps were tested first by Quality testing team in test environment. After confirmation & successful implementation, these are being implemented in production/ live environment. For branches & other division Help Desk software is under development to track the whole problem resolution process and time for resolution. After its deployment, Branch manager will be able to monitor the status & rectification process for the reported problems. These databases can be used for knowledge base information for new users.

Chapter 3

3. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Other risks Bank 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. 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 shall form an ICT Risk Management Committee to govern overall ICT risks and relevant mitigation measures.

3.1.2 The Bank shall define the *Risk Appetite* (amount of risk the Bank 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 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 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 shall define the risk responsibilities to individuals for ensuring successful completion.

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

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

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

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

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

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

3.3.6 The Bank 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 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 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 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 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 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 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 may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. The Bank 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 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 shall form an *ICT Emergency Response Team*, comprising staff within the Bank 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 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 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 .

4.2.8 As incidents may trail from numerous factors, Bank shall perform a root-cause and impact analysis for major incidents which result in severe disruption of ICT services. The Bank 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 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 shall establish a process to log the information system related problems.

4.3.2 The Bank 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 shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.

4.4.2 The Bank 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 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.

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

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

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

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

5.1.11 Bank 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 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 .

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 .

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 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 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 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 ;
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 .
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 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 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 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 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 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 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 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 shall limit access to DC to authorized staff only. The Bank 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 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 shall ensure that the perimeter of the DC, facility and equipment room are physically secured and monitored. The Bank 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 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.

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 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 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 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 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 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 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 shall establish redundant communication links for WAN connectivity.

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

5.8.2 The Bank 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 crypto period. The Bank shall define the appropriate cryptoperiod for each cryptographic key considering sensitivity of data and operational criticality.

5.8.5 The Bank 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 shall ensure that these keys are not exposed during usage and transmission.

5.8.7 When cryptographic keys have expired, the Bank 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 shall generate the new key independently from the previous key.

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

5.9 Malicious Code Protection

5.9.1 The environment of Banks s 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 may arrange awareness program for the end users about computer viruses and their prevention mechanism.

5.10 Internet Access Management

Branch:

1. Highest two PC (recommended one) can have limited internet access for only business purpose.
2. In AD branches the number of pc can increase depends on business purpose to access the internet.
3. All social networking, video streaming, torrent etc. sites should blocked by the capacity and fractures of the internet access devices of the bank.
4. The swift pc can never access the internet.
5. It is recommended to never access CBS and other banking application from the internet pc.
6. Only one pc from each braches is allowed to access USB pen drive.

7. Each branch should be a unique email address for business corresponds and the email password should preserve by two person of the branch. However if personal email address is required for any branch employee for business purpose then he should apply for a valid reason.
8. There is no Wi-Fi connection in the branch to access the BCBL network.
9. Each branch should carry a USB modem. It will use in case of both link failure of the branch. At that time only one pc can access the business applications.
10. The user password should be change once in every thirty days.
11. User must be login to workstation by with won credential.

Head office

1. Only designated user can access internet for limited purpose.
2. All social networking, video streaming, torrent etc. sites should blocked by the capacity and fractures of internet gateway devices.
3. USB pen drive allow in one pc in each department.
4. Each department should be a unique email address for business corresponds and the email password should preserve by two person of the department. However if personal email address is required for any person for business purpose then he should apply for a valid reason.
5. The Wi-Fi device can place in head office for only access internet for high official.
   The user password should be change once in every thirty days.

5.11 Email Management

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

5.11.2 Email system shall be used according to the Bank's policy:

a) The Bank shall provide e-mail ID to employee to enable them to communicate effectively and efficiently with other members of staff, other organizations and banks.

b) When using the Bank's e-mail facilities employee should comply with the following guidelines

- Check e-mail daily at least twice to see if there is any message.
- Include a meaningful subject line the message.
- Check the address line before sending a message and check that you are sending it to the right person.
- Delete e-mail messages when they are no longer required.
- Respect the legal protections to data and software provided by copyright and licenses.
- Take care not to express views, which could be regarded as defamatory or libelous.
- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.

- Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator or authority.
- Do not use e-mail for personal reasons.
- Do not send excessively large electronic mail messages or attachments.
- Avoid flooding. Do not send unnecessary messages such as festive greetings or other non-work items by electronic mail, particularly to several people. Do not participate in chain or pyramid messages or similar schemes.
- Do not represent yourself as another person. Be aware of using your original identity.

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 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 must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

5.11.9Concerned department shall perform regular review and monitoring of e-mail service.

5.11.10All attachments with the incoming e-mail messages shall be monitored especially for viruses.

5.11.11Mail server must have latest anti-virus and anti-spam signature.

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 shall conduct VAs regularly to detect security vulnerabilities in the ICT environment.

5.12.2 The Bank 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 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 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 shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

5.12 Patch Management

5.13.1 The Bank 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 shall establish the implementation timeframe for each category of security patches.

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

5.14 Security Monitoring

5.14.1 The Bank 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 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 against network intrusion attacks as well as provide alerts when an intrusion occurs.

5.14.3 The Bank 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 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 shall only grant access rights and system privileges based on job responsibility. The Bank 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 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 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 shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

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

6.2 Password Management

6.2.1 The Bank 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 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 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;

Chapter 7

Business Continuity and Disaster Recovery Plan

Business Continuity Plan (BCP) is required to cover operational risks and takes into account the potential for wide area disasters, Data Center disasters and the recovery plan. The primary objective of BCP is to enable a bank to survive a disaster and to re-establish normal business operations. In order to survive, we will 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. Success of business continuity depends on how quickly disaster is recovered.

BCP addresses the backup, recovery and restore process. Keeping this into consideration, this chapter covers Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) for centralized operation and Backup and Restore Plan (BRP) for distributed operation.

7.1 Business Continuity Plan (BCP)

The Business Continuity Plan (BCP) covers operational risks keeping in view the potential for WAN disasters, data center disasters and the recovery plan. The BCP also take into consideration the backup and recovery process.

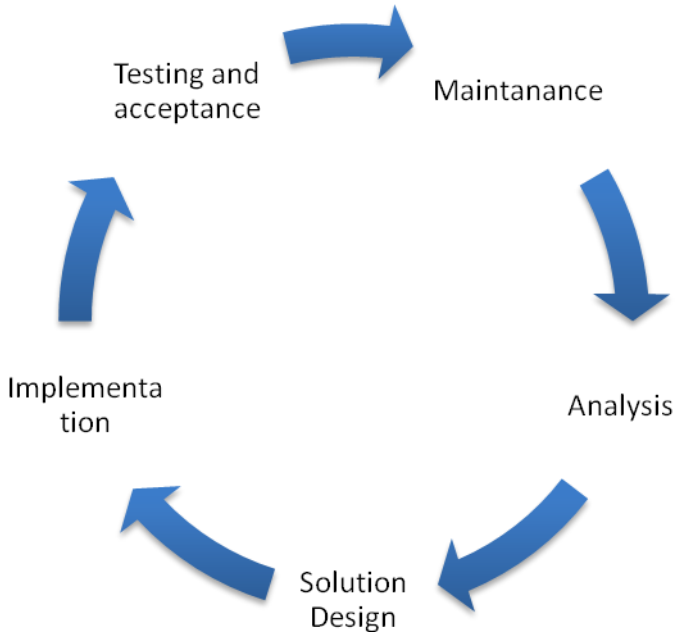
The purpose of the BCP is to establish the rules for recovering data in case of any failure to run the system with a minimum down time.

Following situations are considered to restore business operations within the required time frame:

a) During office hour's disaster

b) Outside office hour's disaster and

c) Immediate and long term plan



Action plans covers:

- Emergency contacts, addresses and phone numbers including venders
- Grab list of items such as backup tapes, laptops, flash drives etc.
- BCP must be tested and reviewed regularly to ensure the effectiveness.

7.1.1 BCP Policy

a) A Business Continuity Team will be formed time to time for a particular period consisting of System Administrator, Network Administrator, Database Administrator and other persons from respective sections. The Head of IT will be the coordinator of the team.

b) Emergency contacts, address and phone numbers including list of vendors should be kept in Data Center, DR Site and branches.

c) Grab list of items such as backup tapes, laptop etc. should be kept in Data Centre, DR Site and branches.

d) Review of BCP must be done at least once a year.

7.1.2 Action Plan

i. The persons on duty at Data Center during and after office time must inform the Head of IT immediately if any business discontinuity happens.

ii. If this happens at branch level, the branch manager will inform the Head of IT immediately.

iii. The Head of IT will call/ inform the Business Continuity Team members and will take necessary actions as describe below.

- **Data Center level Business Continuity:**

a) If, Hardware /Server crashes:

i. **The crashed hardware server will be replaced immediately by the backup server.**

Backup server is always ready for all patch update.

i. **All required software must be pre-installed in the backup server.**

ii. **All the data of the Bank is stored in external storage.**

iii. **Backup server will be mounted in external storage immediately. The process of mount and dismount and other task are already documented.**

iv. **All the data of the bank is copied for redundancy through synchronous replication from DC SAN (Data center storage area network) to DR SAN (Disaster recovery storage area network).**

v. **If DC site fails, then immediately DR site takes place. Usually it takes minimum 1 hour time and maximum 3 hours time to make ready for running the business operation.**

vi. **The whole replication process from SAN to SAN replication is fully documented.**

b) If, Network fails:

i. The backup communication link must be established immediately.

ii. If any network equipment devices crashed then the crashed equipment will be replaced by compatible backup equipment immediately.

iii. **Every core device like core router, core switch, core firewall has redundancy, if one fails other is up immediately.**

iv. The configuration backup of every network device is taken on regular-basis.

- **Branch Level Business Continuity**

a) If, Hardware crashes:

i. The crashed hardware will be replaced immediately by the backup

ii. All required software must be pre-installed in the backup hardware.

b) If, Network fails:

i. The backup communication link must be established immediately.

ii. If any network equipment devices crashed then the crashed equipment

will be replaced by backup equipment immediately**.**

iii. **if both the link is down then the branch's business operation is run by internet modem from one or two PC.**

iv. Among the two network devices (switch and router) if switch fails then the unused ports of the router is configured as switch and the workstations are connected to the router.

v. if router fails then backup router is provided immediately from Head Office. By this time the business is run through internet modem.

7.2 Disaster Recovery Plan (DRP)

- A Disaster Recovery Site (DRS) must be in place replicating the Data Center (Production Site).
- DR site must be at a minimum of 10 kilometers (radius) of distance from the 'production' site.
- DR site shall be equipped with compatible hardware and telecommunication equipment to support the critical services of the business operation in the event of a disaster.
- Physical and environmental security of the DR site shall be maintained.
- Information security shall be maintained properly throughout the recovery process.
- An up-to-date and tested copy of the DR plan shall be securely held off-site. DR plan shall exist for all the critical services where DR requirement is approved by the business.
- DR test shall be carried out successfully at least once a year.
- DR test documentation shall include at a minimum:

  a) Scope, b) Plan, and c) Test Result

7.3 Backup and Restore Plan (BRP)

There shall be a documented backup procedure.

Bank shall ensure the safety and security of the backup copies of information from not being damaged by natural calamities and theft (if possible to be sent at off-site location).

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

The backup shall be done periodically considering the cycle of:

a) Weekly, b) Monthly, c) Yearly or as required by regulatory authority.

The backup log sheet shall be maintained, checked & signed by supervisor.

The backup inventory shall be maintained, checked & signed by supervisor.

The ability to restore from backup media shall be tested at least quarterly.

Backup media must be labeled (soft/hard format) properly indicating contents, date etc.

Chapter 8

8. Acquisition and Development of Information Systems

For any new application of business function for the Bank 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 shall identify system deficiencies and defects at the system design, development and testing phases. The Bank 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 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 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 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 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 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 .

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 .

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 shall have legal licenses and record of the same shall be maintained by the respective unit/department of the Bank .

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 shall consider putting in place the following measures to counteract fraudsters' attacks on ATMs and POS devices:

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

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

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

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

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

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

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

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

9.1.12 The Bank 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 shall educate its customers on security measures that are put in place by the Bank 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 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 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 The Bank shall formulate Internet Banking Security policy considering technology security aspects as well as operational issues:

Internet Banking Policy:

a) Savings, Current, SND account etc. customers can be registered to enjoy BCB Internet Banking service.

b) Jointly operated accounts will not be entitled to enjoy the Internet Banking Service

c) 2-FA (two-factor authentication) must be implemented in the Internet banking transaction.

d) Reputed International SSL certification like Symantec (Verisign), Thoughty, Godaddy etc. must be incorporated in the Internet Banking system to secure and protect the integrity of customers data and system and to enhance confidence in this service.

e) Internet Banking session must be automatically terminated after a fixed period of time unless customer is re-authenticated for the existing session.

f) Monitoring and surveillance systems should be implemented for tracking subsequently any abnormal system activities or unusual transactions.

g) All the activities including all transactions, system accesses, messages received will be logged.

h) To secure Internet banking system & customers data strong security features like Intrusion Prevention System (IPS) must be incorporated in core network equipments like core firewall in the Internet banking backend host system and Intrusion Prevention System (IPS) & Unified Threatkey Management (UTM) must be incorporated in the Internet Banking application server zone to prevent denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack), man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

i) The ICT security unit and External auditors (Licensed penetration tester shall undertake periodic penetration tests of the system.

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 which provides payment card services shall implement adequate safeguards to protect sensitive payment card data. The Bank 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 shall ensure that the processing of sensitive or confidential information is done in a secure environment.

9.3.3 The Bank 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 shall ensure that adequate controls are implemented to manage these transactions.

9.3.4 The Bank shall perform (not a third party payment processing service provider) the authentication of customers' sensitive static information, such as PINs or passwords. The Bank 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 shall ensure that security controls are implemented at payment card systems and networks. Bank 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 shall only activate new payment cards upon obtaining the customer's instruction.

9.3.9 The Bank 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 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 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 shall implement solution to follow up on transactions exhibiting behavior which deviates significantly from a cardholder's usual card usage patterns. The Bank 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 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 s 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 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 shall conduct periodic risk management analysis and security assessment of the MFS operation and take appropriate measures accordingly.

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

Besides these a separate Mobile Banking policy has to be formulated.

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 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 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 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 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 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 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 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 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 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 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).
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 . 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 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).

11.1.5The Bank 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 , E-mails 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.

Chapter 12

IT asset Disposal Policy

1. **Objective**

To minimize security risks associated with equipment disposal through ensuring the secure destruction of discarded data stores.

2. **Scope**

All ICT Facilities and Infrastructure of BCBL.

3. Procedure

Step	Details	Responsibility
1.	Disposal of ICT Assets is the responsibility of the custodian, or manager, of the asset. Prior to disposal, the following should be considered: • Re-deployment options • Asset value and cost recovery • Recycling options • Destruction of data and configuration information prior to disposal	**IT Establishment in-charge**
2.	The ICT Asset disposal process used will be based on an assessment of the data value performed by the responsible parties. **T**he disposal methods presented in this Procedure are intended as a minimum standard of operation; not as directive statements. Workstations that hold critical information stores, for example, can be destroyed using processes of higher diligence than those described in this Procedure.	**IT Establishment in-charge**
3.	In cases where an ICT Asset holds data, the following is considered a reasonable attempt to securely delete data: **Workstations:** Where Branch and Head Office computers are being disposed of, a reasonable attempt to remove data is considered to be: • An operation which overwrites data on the device equivalent to overwriting a device with binary zeroes or random data under Windows/Linux. • Re-installation of an operating system on the	**IT Establishment in-charge**

	drive. **System components:** In cases where an ICT Service is being decommissioned, and the data storage devices will be reused: • An operation which overwrites data on the device equivalent to overwriting a device with binary zeroes or random data under Windows/Linux. •Re-installation of an operating system on the drive prior to redeployment **Scrapped devices:** Where a data storage device will be scrapped: • If the device is functional, an operation which overwrites data on the device must be performed **or** equivalent to overwriting a device with binary zeroes or random data under Windows/Linux. • The data storage device should be destroyed in such a way that reading the device is no longer possible: o Destroying the platters of a hard drive o Destruction of tape media o Using a magnetic field to remove data	

Annexure 1

Dispensation Form

Reference: **Date:**

Section I: Requester Information

Bank Name:

Branch/Division Name:

Requested by:

Requestor's Designation:

Requestor's Telephone:

Request Date:

Section II: Risk Overview

Guideline reference (Clause) and description:
…….
……..
Risk Details (Process/Application/System/Product):
……..
……..
Justification: ……
Plan of mitigation:
……..
……..
Mitigation Date:

Section III: Approvals

The undersigned agree and accept the risk documented on this form.

Name:

Designation:

Comments:

Date:

Signature & Seal:

Annexure 2

Change Request Form

Reference: Date:

Section I : Requester Information

Branch/Division Name:
Submitted by:
Change Description:

Change Purpose:

Request Date:

Section II: Approvals

The undersigned agree and accept the change documented on this form.

Name:
Designation:

Comments:

Date:

Signature & Seal:

Section III: Implementer Details
The undersigned has implemented the requested change on this form.

Change Reference No.:

Date of Change Implementation:

Change Implementation Details:

Was change successful? Yes No

Name:
Designation:

Signature & Seal:

Signature & Seal
(Requester)

Signature & Seal
(Head of Branch/Division)

Annexure 3

User Acceptance Test (UAT)

Reference: **Date:**

Application/System Name:

Change Request Reference: Date:

Test Scope (Detail plan of test):

……..

……

Expected Result:

Actual Result:

User Acceptance Test Fail Success

Comments:

Signature & Seal:

Annexure 4

Request Form

Reference: **Date:**

Section I: Requester Information

Branch/Division Name:

Submitted by:

Contact No. :

Request Details:

Justification:

Request Date:

Section II: Approvals
The undersigned agree and accept the change documented on this form.
Name:
Designation:
Comments:
Date:
Signature & Seal:

Section III: Implementer Details

The undersigned has implemented the requested change on this form.

Request Reference No.:

Date of Request Implementation:

Request Implementation Details:

Was Request done successfully?

Yes
No

Name:

Designation:

Signature & Seal:

Annexure 5

IP Phone Request Form

Date:___/___/201__

Name of the Employee :

Employee ID :

Active Directory User Name :

Designation :

Department :

Branch :

Communication Mail ID :

Contact Number :

Desired Outgoing Type : ☐Local Ext. (Within BCBL) ☐NWD

Desired IP Phone Type : ☐PC Soft Phone ☐IP Phone ☐IP Video Phone

---

Signature of the Employee

Authorization Signature

Date:

IP Phone Ext: __ __ __ __ IP: _____. _____ . _____ . _____ IP Phone Model: __ __ __ __ __ __ __ _

Annexure-6

Organogram