ICT Security Policy
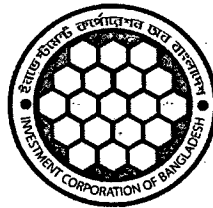
Version 2.0 | 2021

Investment Corporation of Bangladesh

www.icb.gov.bd

Table of Contents

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Preface

New age business environment is very dynamic and undergoes rapid changes as a result of technological innovation, increased awareness and demands from customers. Business organizations, especially the banks and financial institutions of the 21st century operates in a complex and competitive environment characterized by these changing conditions and highly unpredictable economic climate. Information and Communication Technology (ICT) is at the center of this global change.

The application of information and communication technology concepts, techniques, policies and implementation strategies to banking and financial services has become a subject of fundamental importance and concerns to all banks and financial institutions and indeed a prerequisite for local and global competitiveness. As a result of globalization, the deployment of ICT in the financial sector has increasingly become an essential factor for business development and a platform for gaining competitive advantage, especially in a highly competitive industry like investment banking. ICT directly affects how managers decide, how they plan and what products and services are offered. A reliable computer-based information system is essential for efficient management and operation of all the areas of the organization.

The security issue is of special concern in the Banking and Financial institutions, as this industry is highly based on trust from its customers. Hence, the risk of hackers, denial of service attacks, technological failures, breach of privacy of customer information, and opportunities for fraud created by the anonymity of the parties to electronic transactions all have to be managed. Depending upon its nature and scope, a breach in security can seriously damage public confidence in the stability of a financial institution or of a nation's entire banking system. Hence, by introducing the appropriate security measures and putting security concerns at ease, ICB will be able to deliver online services to its large number of customers. Furthermore, it is also in the institution's own interest to improve security, as digital fraud can be costly both in financial losses, and in terms of the damage it does to the brand of the institution in question.

Guidelines covered in this policy are strictly to be followed at all levels in the ICB. It is expected that all possible arrangements be made to implement this ICT Policy. All employees of ICB are required to read this policy carefully and follow the policies and procedures meticulously. This ICT policy may be revised and updated as and when felt necessary by ICB. Furthermore, this Policy will be synchronized with the Policies and / or guidelines to be declared by the Government of Bangladesh or Bangladesh Bank from time to time.

Chapter 1

1.   ICT Security Policy: Scope, Objectives and Applicability

Information Security policy is broadly concerned with the protection of Information resources from unauthorized use or accidental modification, loss or release. Information Security is based on the following five elements:

- **Confidentiality** - ensuring that Information is only accessible to those with authorized access.
- **Integrity** - safeguarding the accuracy and completeness of Information and processing methods.
- **Availability** - ensuring that authorized Users have access to Information when required.
- **Compliant Use** - ensuring that ICB meets all legal and contractual obligations.
- **Responsible Use** - ensuring that appropriate controls are in place so that users have access to accurate, relevant and timely Information but that users shall maintain high ethical standard using ICT Systems.

This policy articulates the principle of conforming to all statutory, legal, regulatory, industry and internal compliance obligations and requirements with respect to the use of Information and Communications Technology (ICT) for conducting business. It defines the context and scope of authorities that are obliged to adhere to whole of ICT contract, Policy, Standard, Notification or equivalent instruction, and provides relevant perspective on the ICB's compliance responsibility for a uniform approach to promoting a compliance culture in support of sound corporate governance of ICT.

1.1   Scope of the Policy

This ICT Policy document applies to all level of officers of ICB, staffs of ICB, all other granted users of ICB's ICT assets and define their responsibility for protection and appropriate use of information, applications, computer system and network. It applies to all ICT domains within ICB and include those domains managed centrally as well as those managed within different branch offices. The policy applies to all subsidiary companies to the extent that they use ICT asset of ICB.

If any matter related to ICT Security is not covered by the policy, it shall be accomplished according to the guideline of the GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL (GOBISM).

1.2   Objectives

The objectives of this ICT Security Policy define the minimum resource requirements, rules, regulations, procedures, security guidelines etc., which the Organization / Institution must adhere to. The objectives are:

1.2.1   To establish a standard ICT Security Policy and ICT Security Management approach

1.2.2   To set up a secure, sustainable and efficient ICT platform.

1.2.3   To establish a secure environment for the processing of data.

1.2.4   To establish a holistic approach for ICT Risk management.

1.2.5   To aware stakeholders' roles and responsibilities for the protection of information.

1.2.6   To prioritize information and ICT systems and associated risks those need to be mitigated.

1.2.7   To establish appropriate project management approach for ICT projects.

1.2.8   To aware and train the users associated with ICT activities for achieving the business objectives.

1.2.9   To define procedure for periodic review of the policy.

1.2.10   To ensure the best practices (industry standard) of the usage of technology that is not limited to this Policy.

1.2.11   To analyze security risks against faster adoption of Bring-Your-Own-Devices (BYOD) .

1.2.12   To minimize security risks for online transactions, mobile financial services etc.

1.3   Applicability of the Policy

This ICT Security Policy is a systematic approach of controls to policies required to be formulated for ensuring security of information and ICT systems. This Policy covers all information that are electronically generated, received, stored, replicated, printed, scanned or manually prepared. The provisions of this Policy are applicable for: all activities and operations required to ensure data security including facility design, physical security, application security, network security, ICT risk management, project management, infrastructure security management, service delivery management, disaster recovery and business continuity management, alternative delivery channels management, acquisition and development of information systems, usage of hardware and software, disposal policy and protection of copyrights and other intellectual property rights

1.4   Categorization of Head office / branches / units depending on ICT Operation

The locations for which the ICT Security Policy is applicable i.e., the Head Office, Branch and/ or Unit of the organization may be categorized into three tiers depending on their ICT setup and operational environment/procedures as:

Tier-1: Centralized ICT Operation through Data Center (DC) including Disaster Recovery Site (DRS) to which all other offices, branches are connected through WAN with 24x7 hours attended operation.

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

Tier-3: Head Office, Branch Office having standalone computer(s). The proposed ICT Security Policy will be applicable for all the three tiers if not mentioned otherwise.

Chapter 2

2.   ICT Security Management

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

2.1   Roles and Responsibilities

Well-defined roles and responsibilities of Board and Senior Management are critical while implementing ICT Security Management and Governance. Clearly-defined roles enable effective project control and expectations of organizations. ICT Security Management and Governance stakeholders include Board of Directors, ICT Steering Committee, ICT Security Committee, Risk Management Committee, CIRT Committee, MD, DMD, GM, CISO, CEOs, System Managers, Information Technology Security Managers, System Owners, ICT Security department/division, ICT audit department/division and other related Business department/division.

2.1.1   The Board of Directors

2.1.1.1   Approving ICT strategy and policy documents.

2.1.1.2   Ensuring that the management has placed an effective planning process to establish and maintain a state-of-the-art ICT system and secured ICT management within ICB.

2.1.1.3   Endorsing that the ICT strategy is indeed aligned with business strategy.

2.1.1.4   Ensuring that the ICT organizational structure complements the business model and its direction. ICT organizational structure and ICT Infrastructure shall be planned, implemented and updated regularly to ensure standardized, up-to-date and secured ICT operations.

2.1.1.5   Ensuring ICT investments represent a balance of risks and benefits and acceptable budgets.

2.1.1.6   Ensure compliance status of ICT Security Policy.

2.1.2   The Managing Director

The Managing Director as the agency head endorses and is accountable for information security within ICB. The Managing Director is the highest Accreditation Authority for ICB. When the Managing Director chooses to delegate his/her authority as ICB's Accreditation Authority He/she shall do so with careful consideration of all the associate risks, as they remain responsible for the decisions made by their delegate. The Chief Information Security Officer (CISO) is the most appropriate choice for delegated authority as they shall be a senior management and hold specialized knowledge in information security and security risk management.

2.1.2.1   The Managing Director as the agency head endorses and is accountable for information security within ICB. The Managing Director is the highest Accreditation Authority for ICB.

2.1.2.2   Where the Managing Director devolves his/her authority, the delegate must be at least a member of the Senior Management Team or an equivalent management position. The Chief Information Security Officer (CISO) is the most appropriate choice for delegated authority

2.1.2.3   The Managing Director shall provide full support for the proper development, implementation and maintenance of information security processes, infrastructure and operations within ICB.

2.1.2.4   The Managing Director shall provide full support to plan, implement and regularly update ICT organizational structure, ICT Infrastructure, ICT Processes and ICT security policy to ensure standardized, up-to-date and secured ICT operations within ICB.

2.1.3   ICT Steering Committee

ICT Steering Committee needs to be formed with representatives from Senior Management, ICT operations, ICT security, ICT Infrastructure, ICT Development, ICT audit/Compliance, Risk, HR, Legal and other related Business units.

2.1.3.1   Recommend necessary action procedures to perform all ICT related activities and monitor management methods to determine and achieve strategic goals

2.1.3.2   Aware about exposure towards ICT risks and controls

2.1.3.3   Provide guidance related to risk, funding, or sourcing

2.1.3.4   Ensure project priorities and assessing feasibility for ICT proposals

2.1.3.5   Ensure that all critical projects have a component for "project risk management"

2.1.3.6   Consult and advice on the selection of technology within standards & monitor establishment, implementation and operation thereto.

2.1.3.7   Ensure that vulnerability assessments of new technology is performed

2.1.3.8   Ensure compliance to regulatory and statutory requirements

2.1.3.9   Provide direction to architecture design and ensure that the ICT architecture reflects the need for legislative and regulatory compliance

2.1.3.10   To cope with growing demand, ICT Management Structure has been changing and expanding both horizontally and vertically with the enhanced manpower.

2.1.3.11   Recommend and advice on development/modification/upgradation/enhancement of software considering ICT risk.

2.1.3.12   Provide approval of respective requirement and design related to any development/modification /upgradation/enhancement of any software and other ICT systems.

2.1.3.13   Recommend and advice regarding purchase and modification/upgradation/ enhancement of any hardware, software, network system, ICT security system etc.

2.1.4 ICT Security Committee

ICT Security Committee needs to be formed with representative from Senior Management, ICT security, ICT audit/Compliance, ICT operations, ICT Infrastructure, ICT Development, Risk, HR, Legal and other related Business units.

2.1.4.1 Ensure development and implementation of ICT security objectives, ICT security related policies and procedures.

2.1.4.2 Provide ongoing management support to the Information security processes.

2.1.4.3 Ensure continued compliance with the business objectives, regulatory and legal requirements related to ICT security.

2.1.4.4 Support to formulate ICT risk management framework/process and to establish acceptable ICT risk thresholds/ICT risk apatite and assurance requirements.

2.1.4.5 Periodic review and provide approval for modification in ICT Security processes.

2.1.5 CIRT Committee

CIRT committee needs to be formed with representative from Senior Management, ICT security, ICT operation, ICT Infrastructure, ICT Development, ICT audit/Compliance, Risk and other related Business units.

2.1.5.1 Ensuring Monitoring of the servers and the network for any events that can affect the security of ICB's Data and ICT network;

2.1.5.2 Carry out investigations and containment measures for cyber security events in order to minimize data loss or service disruption in the ICB network and e-services;

2.1.5.3 Help to solve security related issues in ICB Data Center;

2.1.5.4 Ensuring preventive measures in order to minimize disruptions of secure operations of the ICB network and e-services;

2.1.5.5 Promote and strengthen cyber security environment by developing, collaborating and maintaining relationships with other CIRT's and organizations in the country and abroad;

2.1.6 The Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) sets the strategic direction for information security. The CISO is responsible for facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within ICB. The CISO is also responsible for providing strategic level guidance for ICB security program and ensuring compliance with national policy, standards, regulations and legislation.
Having the CISO coordinate the use of external information security resources will ensure that a consistent approach is being applied across ICB.

As the CISO is responsible for the overall management of information security within ICB, it is important that they report directly to the Managing Director on any information security issues. To ensure that the CISO is able to accurately report to the MD on information security issues within ICB it is important that they remain fully aware of all information security incidents within ICB.

2.1.6.1   The Chief Information Security Officer (CISO) sets the strategic direction for information security within ICB.

2.1.6.2   ICB shall appoint a person to the role of CISO or have the role undertaken by an existing capable member of the Senior Management Team or an equivalent management position.

2.1.6.3   Where the role of the CISO is outsourced, potential conflicts of interest in availability, response times or working with vendors shall be identified and carefully managed.

2.1.6.4   CISO shall report directly to the Managing Director on matters of information security within ICB.

2.1.6.5   CISO shall develop and maintain a comprehensive strategic level information security and security risk management program within ICB aimed at protecting ICB's information.

2.1.6.6   CISO shall be responsible for the development of an information security communications plan.

2.1.6.7   CISO shall create and facilitate ICB's security risk management process.

2.1.6.8   CISO shall be responsible for ensuring compliance with the information security policies and standards within ICB.

2.1.6.9   CISO shall be responsible for ensuring ICB's compliance with the GOBISM through facilitating a continuous program of certification and accreditation based on security risk management.

2.1.6.10   CISO shall provide strategic level guidance for ICB's ICT projects and operations.

2.1.6.11   CISO shall coordinate the use of external information security resources including contracting and managing the resources.

2.1.6.12   CISO shall be responsible for controlling the information security.

2.1.6.13   CISO shall be fully aware of all information security incidents.

2.1.6.14   CISO shall coordinate the development of disaster recovery policies and standards to ensure that business critical services are supported appropriately and that information security is maintained in the event of a disaster.

2.1.6.15   CISO shall be responsible for overseeing the development and operation of information security awareness and training programs.

2.1.7 Information Technology Security Managers (ITSMs)

Information Technology Security Managers (ITSMs) provide information security leadership and management to support and enforce information security policies. ITSMs are senior executives who act as a conduit between the strategic directions provided by the CISO and the technical efforts. The main area of responsibility of an ITSM is that of the administrative and process controls relating to information security within ICB. As ITSMs are responsible for the operational management of information security projects and functions, they will be aware of their funding requirements and can assist the CISO to develop information security budget projections and resource allocations.

ITSMs are responsible for managing the implementation of information security measures within ICB. To ensure the CISO remains aware of all information security issues within ICB and can brief the Managing Director when necessary, ITSMs will need to provide regular reports on policy developments, proposed system changes and enhancements, information security incidents and other areas of particular concern to the CISO.

Whilst the CISO will coordinate the development of disaster recovery policies and standards, ITSMs will need to guide the selection of appropriate strategies to achieve the direction set by the CISO.

2.1.7.1 Information Technology Security Managers (ITSM) provide information security leadership and management.

2.1.7.2 ICB must have ITSMs for its Information Security management. ITSMs shall be supported by Information Security Division and departments.

2.1.7.3 ITSMs must be responsible for assisting system owners to obtain and maintain the accreditation of their systems

2.1.7.4 ITSMs must be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans, Systems Security Plans and any Standard Operating Procedures (SOPs) for all ICT systems

2.1.7.5 ITSMs shall work with the CISO to develop an information security program within ICB

2.1.7.6 ITSMs shall undertake and manage projects to address identified security risks

2.1.7.7 ITSMs shall identify systems that require security measures and assist in the selection of appropriate information security measures for such systems Recommended Control

2.1.7.8 ITSMs shall consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.

2.1.7.9 ITSMs shall work with system owners, systems certifiers and systems accreditors to determine appropriate information security policies for their systems and ensure consistency with relevant GOBISM components.

2.1.7.10 ITSMs shall notify the Accreditation Authority of any significant change that may affect the accreditation of that system.

2.1.7.11 ITSMs shall liaise with vendors and ICB purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements

2.1.7.12 ITSMs shall conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies, if necessary

2.1.7.13 ITSMs shall select and coordinate the implementation of controls

2.1.7.14 ITSMs shall provide leadership and direction for the integration of information security strategies and architecture with ICB's business and ICT strategies and architecture

2.1.7.15 ITSMs shall provide technical and managerial expertise for the administration of information security management tools

2.1.7.16 ITSMs shall work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives

2.1.7.17 ITSMs shall coordinate, measure and report on technical aspects of information security management to CISO

2.1.7.18 ITSMs shall monitor and report to CISO on compliance with information security policies, as well as the enforcement of information security policies.

2.1.7.19 ITSMs shall monitor and provide regular reports on information security incidents and other areas of particular concern to the CISO

2.1.7.20 ITSMs shall assess and report to CISO on threats, vulnerabilities, and residual security risks and recommend remedial actions

2.1.7.21 ITSMs shall assist system owners and security personnel in understanding and responding to audit failures reported by auditors.

2.1.7.22 ITSMs shall assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans

2.1.7.23 ITSMs shall provide or arrange for the provision of information security awareness and training for all ICB personnel

2.1.7.24 ITSMs shall provide expert guidance on security matters for ICT projects

2.1.7.25 ITSM shall keep the CISO and system owners informed with upto-date information on current threats

2.1.8. System Owners
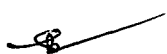
System owner is the nominated of an ICT Asset. System owners obtain and maintain accreditation of their systems. The system owner is responsible for the overall operation of the system and they may delegate the day-to-day management and operation of the system to a responsible manager or managers. System owners need to ensure that systems are accredited to meet ICB's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

All systems shall have a system owner in order to ensure IT governance processes are followed and that business requirements are met. It is strongly recommended that a system owner be a member of the Senior Management Team or in an equivalent management position.

2.1.8.1 System owners obtain and maintain accreditation of their systems

2.1.8.2 Each system must have a system owner who is responsible for the operation and maintenance of the system

2.1.8.3 System owners must obtain and maintain accreditation of their system(s)

2.1.8.4 System owners must ensure the development, maintenance and implementation of complete, accurate and up to date Security Risk Management Plans, Systems Security Plans and Standard Operating Procedures (SOPs) for systems under their ownership. Such actions must be documented.

2.1.8.5 System Owners involve the ITSM in the redevelopment and updates of the SRMPs, SecPlans, and SOPs

2.1.8.6 System owners shall be a member of the Senior Executive Team or an equivalent management position.

2.2 ICT Security Policy (SecPol), Standard and Procedure

2.2.1 ICT Security Policy (SecPol) set the strategic direction for information and ICT systems security.

2.2.2 ICT Security Policy (SecPol) has to be complied with the Guideline of the GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL (GOBISM) and The Guideline on ICT Security for Banks and Non-Bank Financial Institutions published by Bangladesh Bank. The ICT Security Policy (SecPol) has to be approved by the board. The policy covers common technologies such as computers and peripherals, data and network, applications and other specialized ICT resources. ICB's service delivery depends on availability, reliability and integrity of its information technology system. Therefore, appropriate controls to protect its information system must be adopted. The senior management of ICB must express commitment to ICT security by ensuring continuous awareness and training program for each level of staff and stakeholders.

2.2.3 The policy requires regular update to deal with evolving changes in the ICT environment both within ICB and overall industry.

2.2.4   ICT professional shall be employed in separate ICT security division/department/unit, ICT audit department/unit and ICT compliance department/unit for improved and impartial dealing with ICT security management, ICT compliance management, ICT audit, security incident management, ICT Risk management, ICT security policy documentation, inherent ICT risks, risk treatments and other relevant activities.

2.2.5   Certification and Accreditation framework and processes shall be established and placed in operation for auditing, testing, evaluating and authorizing ICT systems/ components/ activities prior to implementation in ICB's ICT system

2.2.6   The Government of Bangladesh Information Security Manual (GOBISM)

2.2.7   For noncompliance issues related to the Guideline on ICT Security for Banks and Non-Bank Financial Institutions published by Bangladesh Bank, compliance plan shall be submitted to Bangladesh Bank for taking dispensation. Dispensation shall be for a specific period of time. (**Annexure- 1: Dispensation Form**)

2.3 Internal Information System Audit

2.3.1   Internal ICT Audit Department shall be established. Adequate personnel shall be placed in the department. Personnel placed in the department shall be trained properly to achieve sufficient Information System (IS) Audit expertise and skills.

2.3.2   Internal Information System (IS) audit shall be carried out by ICT Audit Department of ICB.

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

2.3.4   Computer-Assisted-Auditing Tools (CAATs) to perform IS audit planning, monitoring/auditing, control assessment, data extraction/ analysis, fraud detection/prevention and management might be used.

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

2.3.6   Internal Information System (IS) audit shall be done periodically at least once a year. The report must be preserved for regulators as and when required. It shall be also ensured that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

2.3.7   Appropriate measures shall be taken to address the recommendations made in the last Audit Report (external/internal). This must be documented and kept along with the Audit Report mentioned in 2.5.6.

2.4 External Information System Audit

2.4.1   External IS auditor(s) with sufficient IS Audit expertise and skills shall be engaged for information systems auditing in-line with regular financial audit.

2.4.2   The audit report shall be preserved for regulators as and when required. Appropriate measures shall be taken to address the recommendations made in the last Audit Report.

2.5   Standard Certification

Industry standard certifications shall be obtained related to Software Development, Information System Security, Quality of ICT Service Delivery, Business Continuity Management, Payment Data Security etc.

2.6   Security Awareness and Training

2.6.1   As technology evolves rapidly, it shall be ensured that all relevant ICT personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.

2.6.2   Minimum level of Business Foundation Training shall be provided for ICT personnel.

2.6.3   Information System (IS) security awareness training/workshop shall be arranged for all staff.

2.6.4   Adequate training/awareness facilities shall be ensured for ICT personnel considering any new services and technological changes.

2.7   Insurance or Risk Coverage Fund

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

2.7.2   The risk coverage fund shall be maintained properly in the accounting system of ICB.

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

2.8   Procurement Management

2.8.1   ICT Wing shall develop long and short-term plans for purchasing hardware and software.

2.8.2   Equipment and software shall be procured as per the procurement policy of the Corporation / Public Procurement Rule (PPR).

2.8.3   The ICT Wing shall provide technical support to make purchases of a routine nature that are included in the budget approved in every calendar year by proper authority. Branch Offices may made minor purchases that are budgeted and approved by competent authority.

Chapter 3

ICT Asset and Infrastructure Security Management

ICB's ICT assets includes all the hardware, software, applications, database systems, network devices and technologies within ICB's ICT system. The ICT landscape is vulnerable to various forms of attacks. The frequency and malignancy of such attacks are increasing. It is imperative that ICB implements security solutions at the data, application, database, operating systems, hardware 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.

3.1   ICT Asset Management: General consideration

3.1.1   ICT asset inventory shall be maintained by procuring entity stating significant details (e.g. owner, custodian, purchase date, location, license number, configuration, etc.). **Annexure -4: Stock Register of Hardware and Software.**

3.1.2   Prior to procuring any new ICT assets, compatibility assessment (with existing system) and security assessment shall be performed properly.

3.1.3   All ICT asset procurement shall be complied with the procurement policy of ICB.

3.1.4   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. In case of changing custodian proper handover/takeover shall be done properly. **Annexure -11: Handover/takeover of ICT Asset**

3.1.5   All ICT assets shall be clearly identified and labeled (where possible). Labeling shall reflect the established classification of assets.

3.1.6   In case of movement of ICT assets, a register shall be maintained where detail information of the specific asset movement, its cause, related person's particulars, date and time shall be logged on which must be counter signed by the concerned officer.

3.1.7   The ICT asset inventory shall be reviewed and updated regularly.

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

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

3.1.10 Guidelines shall be provided for the use of portable devices, especially for the usage at outside premises.

3.1.11 There shall be a policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.

3.1.12 The terms of all software/hardware/firmware/device/technology licenses shall be complied with and shall not use any software/hardware/firmware/device/technology that has not been legally purchased or otherwise legitimately obtained.

3.2   Software Controls

3.2.1   For all servers and workstations, a standard configuration shall be created and updated for each operating system type and version.

3.2.2   It shall be ensured that for all servers and workstations installed operating system patching is up to date.

3.2.3   There shall be an approved list of Software applications which will only be used within the ICT system of ICB. This approved list of Software shall be updated regularly.

3.2.4   System users shall not install or uninstall any software without approval.

3.2.5   Use of any unauthorized software shall strictly be prohibited within the ICT system of ICB.

3.2.6   All In-house developed software and application used in production environment in shall be copyrighted.

3.2.7   All the software applications must have proper certification and accreditation prior to deployment in the production environment

3.2.8   All In-house developed software shall have proper change management and version controlling system.

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

3.2.10 Vulnerability Assessment and penetration testing shall be conducted for any **core business operation software** before deployment.

3.2.11 All the **core business operation software** shall have standard and strong password management facility as per password policy.

3.2.12 All the **core business operation software** shall have user management facility, audit logging facility and user activity logging facility.

3.2.13 Audit and other logs of all the **core business operation software** shall be protected through the use of a one-way pipe to reduce likelihood of compromise key transaction records.

3.2.14 All the Financial Transaction entry in any **core business operation software** shall use Maker-checker principle.

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

3.2.16 Source codes/executable files/installation files of software/applications used in production environment shall be properly listed in **Stock Register of Hardware and Software.**

3.2.17 There shall be a Backup and restoration plan for Source codes/executable files/installation files of software/applications used in production environment.

3.2.18 Backup copy of Source codes/executable files/installation files of software/applications used in production environment shall be stored in a safe place as per the Backup and restoration plan.

3.3   Desktop/Laptop Devices Controls

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

3.3.2   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 ICB.

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

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

3.3.5   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.

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

3.3.7   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.

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

3.3.9   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).

3.3.10 Any kind of viruses shall be reported immediately.

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

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

3.3.13 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.

3.3.14 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.)

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

3.4   Server Security Controls

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

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

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

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

3.4.5   Test server(s) shall be maintained to provide a platform for testing of configuration settings, new patches and service packs before applied on the production system.

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

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

3.4.8   All unnecessary programs shall be uninstalled from production servers.

3.4.9   In case of virtualization:

　　　3.4.9.1.   Setting limit on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM shall be planned.

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

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

　　　3.4.9.4.   Synchronized time for host and guests use shall be ensured synchronized time.

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

3.5 Server room/Network Room/Rack Controls

3.5.1 Servers, Network devices (such as router, switch, hub etc.) and Major System security devices (such as firewalls, content filtering devices, penetration testing devices etc.) shall be secured within server room/communications rooms with appropriate physical security.

3.5.2 It must be ensured that keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.

3.5.3 Server rooms, communications rooms or security containers shall not be left in any unsecured state unless the server room is occupied by authorized personnel.

3.5.4 ICB must develop a Site Security Plan (SitePlan) for each server and communications room. Information to be covered includes, but is not limited to:

    3.5.4.1. a summary of the security risk review for the facility the server or communications room is located in

    3.5.4.2. roles and responsibilities of facility and security personnel

    3.5.4.3. the administration, operation and maintenance of the electronic access control system or security alarm system

    3.5.4.4. key management, the enrolment and removal of system users and issuing of personal identification number codes and passwords

    3.5.4.5. regular inspection of the generated audit trails and logs • end of day checks and lockup

    3.5.4.6. reporting of information security incidents

    3.5.4.7. what activities to undertake in response to security alarms

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

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

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

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

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

3.5.10 Patch panels, fiber distribution panels and structured wiring enclosures shall be located within at least lockable commercial cabinets.

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

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

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

3.5.14 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.

3.5.15 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.

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

3.6 Data Center Controls

As critical systems and data of a ICB 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.

3.6.1 Physical Security

3.6.1.1 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.

3.6.1.2 Access to DC shall be limited to authorize staff only. Access to the DC shall only grant on a need to have basis. Physical access of staff to the DC shall be revoked immediately if it is no longer required.

3.6.1.3 Access authorization procedures shall be strictly applied to vendors, service providers, support staff and cleaning crews. Visitors are accompanied at all times by an authorized employee shall be ensured, while in the DC.

3.6.1.4 Access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center. **(Annexure -5: Access Authorization List).**

3.6.1.5 All physical access to sensitive areas must be logged with date, time and purpose shall be maintained for the vendors, service providers and visitors entered into the Data Center **(Annexure -6: Access Log Book and Annexure -7: Visitors Log Book).**

3.6.1.6 It shall be ensured that the perimeter of the DC, facility and equipment room are physically secured and monitored. Physical, human and procedural controls shall be employed for 24 hours such as the use of security guards, card access system, mantraps and surveillance system where appropriate.

3.6.1.7 Emergency exit door shall be available.

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

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

3.6.1.10 If DC is operated by an outsourced service supplier, the contract between ICB and supplier must indicate that all the requirements of Policy regarding physical security must be complied with and that ICB reserves the right to review physical security status at any time.

3.6.1.11 If DC is operated by an outsourced service supplier, the responsibility for physical security lies with the supplier, but access to such facilities dedicated to ICB's use must be reviewed and authorized by ICB.

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

3.6.1.13 Each department is responsible to protect technology resources from unauthorized access in term of both physical hardware and data perspectives.

3.6.2 Environmental Security

3.6.2.1 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.

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

3.6.2.3 Development and test environment shall be separated from production.

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

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

3.6.2.6 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 equipment.

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

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

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

3.6.2.10 Data Center shall have dedicated telephone communication.

3.6.2.11 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.

3.6.2.12 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.

3.6.2.13 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.

3.6.2.14 the following environmental controls shall be installed:

    3.6.2.14.1 Uninterrupted Power Supply (UPS) with backup units

    3.6.2.14.2 Backup Power Supply

    3.6.2.14.3 Temperature and humidity measuring devices

    3.6.2.14.4 Water leakage precautions and water drainage system from Air Conditioner

    3.6.2.14.5 Air conditioners with backup units. Industry standard air conditioning system shall be in place to avoid water leakage from the conventional air conditioning system.

    3.6.2.14.6 Emergency power cut-off switches where applicable

    3.6.2.14.7 Emergency lighting arrangement

    3.6.2.14.8 Dehumidifier for humidity control

3.6.2.15 the above-mentioned environmental controls shall be regularly tested and maintenance service contract shall be for 24x7 bases.

3.6.3 Fire Prevention

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

3.6.3.2 Fire suppression equipment shall be installed and tested periodically.

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

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

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

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

3.7   Networks Security Management

3.7.1   A secured ICT network shall be designed, properly documented and configured by expert professionals. The network design shall be properly certified and accredited before implementation.

3.7.2   For each ICT network ICB manages, there shall be

   3.7.2.1.   a high-level diagram showing all connections and gateways into the network

   3.7.2.2.   a network diagram showing all communications equipment

3.7.3   ICB's ICT network diagrams shall illustrate all network devices including firewalls, IDSs, IPSs, routers, switches, hubs, etc. It does not need to illustrate all IT equipment on the network, such as workstations or printers which can be collectively represented.

3.7.4   Any change to the design and configuration of ICT networks shall be accredited/authorized and shall be controlled through appropriate change management processes to ensure security, functionality and capability is maintained.

3.7.5   All changes to the network configuration shall be documented properly.

3.7.6   ICBs shall keep the network configuration under the control of a network management authority

3.7.7   Baseline standards shall be established to ensure security for Operating Systems, Databases, Network equipment and portable devices which shall meet organization's policy.

3.7.8   Regular enforcement checks shall be conducted to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation.

3.7.9   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.

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

3.7.11   Physical security of all network equipment shall be ensured.

3.7.12   A security risk assessment must be performed before providing network documentation to a third party, such as a commercial provider or contractor.

3.7.13   Network documentation provided to a third party, such as to a commercial provider or contractor, must contain only the information necessary for them to undertake their contractual services and functions, in line with the need-to-know principle.

3.7.14   Detailed network configuration information must not be published in tender documentation.

3.7.15   Wireless local area networks shall be deployed in a secure manner that does not compromise the security of information and systems (as per GOBISM).

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

3.7.17   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.

3.7.18   Network security devices shall be installed, such as firewalls as well as intrusion detection and prevention systems, at critical stages of its ICT infrastructure to protect the network perimeters.

3.7.19 Firewalls or other similar measures shall be deployed, 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.

3.7.20 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.

3.7.21 Rules on network security devices shall be Backup and reviewed on a regular basis to determine that such rules are appropriate and relevant.

3.7.22 Redundant communication links for WAN connectivity shall be established.

3.7.23 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.

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

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

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

3.7.27 Regular network log monitoring and analysis system shall be established

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

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

3.7.30 All default passwords of network devices shall be changed.

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

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

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

3.8 Security Monitoring

3.8.1 ICT Security Division/Department/Unit shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.

3.8.2 Network surveillance and security monitoring procedures shall be implemented with the use of network security devices, such as intrusion detection and prevention systems, to protect ICB against network intrusion attacks as well as provide alerts when an intrusion occurs.

3.8.3 ICT Security Division/Department/Unit 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.

3.8.4 ICT Security Division/Department/Unit 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.

3.8.5 Network Monitoring center (NOC) and Security Monitoring Center (SOC) shall be established comprised of educate and skilled personnel.

3.9 Intrusion Detection and Prevention

3.9.1 Intrusion Detection and Prevention Systems (IDS / IPS) shall be placed in ICB's ICT network.

3.9.2 When signature-based intrusion detection is used, the signatures and system patching must be kept up to date.

3.9.3 It shall be ensured that sufficient resources are provided for the maintenance and monitoring of IDS/IPS

3.9.4 IDS/IPSs shall be deployed in all gateways between ICB's networks and unsecure public networks or BYOD wireless networks

3.9.5 IDS/IPSs rule sets shall be tested prior to implementation to ensure that they perform as expected.

3.9.6 Proper and authorized tools shall be procured and used for managing and monitoring IDS/IPS

3.10 Firewalls

3.10.1 All gateways must contain a firewall in both physical and virtual environment

3.10.2 Firewalls shall be deployed, 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.

3.10.3 The requirement to implement a firewall as part of gateway architecture must be met independently by both parties (gateways) in both physical and virtual environments. (Shared equipment DOES not satisfy the requirements of this control)

3.11 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. There shall be aware of the heightened security risks associated with BYOD due to challenges in securing, monitoring and controlling employees' personal devices.

3.11.1 A comprehensive risk assessment shall be conducted on the BYOD implementation to ensure that measures adopted sufficiently to mitigate the security risks associated with BYOD.

3.11.2 The BYOD implementation shall not be proceeded with if they are unable to adequately manage the associated security risks.

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

3.11.3.1 Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs);

3.11.3.2 Incidents involving threats to, or compromise of, the ICT infrastructure and other information assets (e.g. malware infection or hacking) of ICB;

3.11.3.3 Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);

3.11.3.4 Intellectual property rights for information created, stored, processed or communicated on PODs in the course of work for the ICB.

3.11.4 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 ICB's networks by failing to secure their own equipment.

3.11.5 Appropriate forms of device authentication shall be implemented for PODs approved by authority, such as digital certificates created for each specific device.

3.11.6 ICB has the right to control its information. This must include the right to backup, retrieve, modify, determine access and/or delete ICB's data without reference to the owner or user of the POD.

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

3.11.8 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 ICB's data and technology infrastructure.

3.12 Cryptography

The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is commonly used in ICB 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.

3.12.1 Cryptographic key management policy and procedures shall be established covering generation, distribution, installation, renewal, revocation and expiry

3.12.2 It shall be ensured 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.

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

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

3.12.5 It shall be ensured that hardware security modules and keying materials are physically and logically protected.

3.12.6 When cryptographic keys are being used or transmitted, it shall be ensured that these keys are not exposed during usage and transmission.

3.12.7 When cryptographic keys have expired, a secure key destruction method shall be used to ensure keys could not be recovered by any parties.

3.12.8 In the event of changing a cryptographic key, the new key shall be generated independently from the previous key.

3.12.9 A backup of cryptographic keys shall be maintained. The same level of protection as the original cryptographic keys shall be accorded to backup keys.

3.12.10   if a key is compromised, it shall be immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. All parties concerned of the revocation of the compromised keys shall be informed.

3.13   Malicious Code Protection

3.13.1   The environment of ICB's including servers and workstations must be protected from malicious code by ensuring that approved anti-virus packages are installed.

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

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

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

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

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

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

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

3.13.9   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.

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

3.13.11   Awareness program shall be arranged for the end users about computer viruses and their prevention mechanism.

3.14   Internet Access Management

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

3.14.2   Access to and use of the internet from ICB premises must be secure and must not compromise information security of ICB.

3.14.3   Access to the Internet from ICB premises and systems must be routed through secure gateways.

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

3.14.5   Employees shall be prohibited from establishing their own connection to the Internet using ICB's systems or Devices.

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

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

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

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

3.15   Email Management

3.15.1   Email system shall be used according to the ICB's policy.

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

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

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

3.15.5   Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of ICB, 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.

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

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

3.15.8   Email transmissions from ICB   must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

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

3.15.10   Personnel shall not click on active Web Addresses within email they receive.

3.16   Vulnerability Assessment and Penetration Testing

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

3.16.1   Vulnerability analysis strategy shall be established by:

       3.16.1.1   monitoring public domain information about new vulnerabilities in operating systems and application software

       3.16.1.2   considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner

       3.16.1.3   running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented

       3.16.1.4   using security checklists for operating systems and common applications

       3.16.1.5   examining any significant incidents on the agency's system

3.16.2   Vulnerability assessments shall be conducted in order to establish a baseline:

       3.16.2.1   before a system is first used

       3.16.2.2   after any significant incident

       3.16.2.3   after a significant change to the system

       3.16.2.4   after changes to standards, policies and guidelines

       3.16.2.5   as specified by an ITSM or the system owner

3.16.3   VAs shall be conducted regularly to detect security vulnerabilities in the ICT environment.

3.16.4   A combination of automated tools and manual techniques shall be deployed 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.

3.16.5   A process shall be established to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

3.16.6   Penetration tests shall be carried out in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. Penetration tests shall be conducted on network infrastructure and internet-based systems periodically or need basis.

3.17   Patch Management

3.17.1   The patch management procedures shall be established and ensured, including identification, categorization and prioritization of security patches. To implement security patches in a timely manner, the implementation timeframe shall be established for each category of security patches.

3.17.2   Rigorous testing of security patches shall be performed before deployment into the production environment.

Chapter 4

4. Access Control of Information System

Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems. Access rights and system privileges shall be granted based on job responsibility. It shall be checked 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.

4.1   User Access control

4.1.1   User access to ICT systems and networks shall be granted only on a need-to-use basis and within the period when the access is required.

4.1.2   A set of policies and procedures shall be developed covering system users' identification, authentication and authorization.

4.1.3   For ICB's own software systems, a set of policies and procedures shall be developed to grant, revoke or manage 'user access' and 'user role', considering data security with importance.

4.1.4   It must be ensured that all system users are uniquely identifiable and authenticated on each occasion that access is granted to a system.

4.1.5   Numerical passwords (or personal identification number) must not be used as the sole method of authenticating a system user to access a system.

4.1.6   Storage of unprotected authentication information must not be allowed that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access.

4.1.7   It must be ensured that system users provide sufficient evidence to verify their identity when requesting a password reset for their system account

4.1.8   Shared credentials must not be used to access any account.

4.1.9   Non-employees (contractual, outsourced, or vendor staff) shall be closely monitored for access restrictions.

4.1.10   Each user must have a unique User ID and a valid password to access any of ICB's ICT system.

4.1.11   User ID Maintenance form with access privileges shall be duly approved by the appropriate authority. **(Annexure -8 : User Creation Form).**

4.1.12   User access shall be locked for maximum 3 consecutive unsuccessful login attempts.

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

4.1.14   It shall be ensured that records of user access are uniquely identified and logged for audit and review purposes.

4.1.15   Regular reviews of user access privileges shall be performed to verify that privileges are granted appropriately.

4.2   Password Management

4.2.1   Strong password controls over users' access shall be enforced.

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

4.2.3   Password definition parameters shall ensure that minimum password length is maintained according to ICB's Policy (at least 10 characters).

4.2.4   password policy shall be implemented enforcing a minimum password length of ten characters, consisting of at least three of the following character sets:

    4.2.4.1.   lowercase characters (a-z)

    4.2.4.2.   uppercase characters (A-Z)

    4.2.4.3.   digits (0-9)

    4.2.4.4.   punctuation and special characters

4.2.5   Maximum validity period of password shall not be beyond 90 days.

4.2.6   System users shall be prevented from changing their password more than once a day

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

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

4.2.9   Administrative passwords of Operating System, Database and Business Applications shall be kept in a safe custody with sealed envelope. (**Annexure -9: Password Handover Form**).

4.2.10   Passwords shall not be stored in the clear on the system

4.3   Input Control

4.3.1   Session time-out period for users shall be set in accordance with ICB's Policy.

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

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

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

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

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

4.4   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.

4.4.1   Stringent selection criteria and thorough screening shall be applied when appointing staff to critical operations and security functions.

4.4.2   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. Following controls and security practices shall be adopted for privileged users:

    4.4.2.1   Implement strong authentication mechanisms;

4.4.2.2   Implement strong controls over remote access;

4.4.2.3   Restrict the number of privileged users;

4.4.2.4   Grant privileged access on a "need-to-have" basis;

4.4.2.5   Review privileged users' activities on a timely basis;

4.4.2.6   Prohibit sharing of privileged accounts;

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

4.5   Responsibilities of Users

4.5.1   Every user must log off before leaving his/ her computer.

4.5.2   Computers and monitors will be turned off at the end of each workday.

4.5.3   Laptop computers actively connected to the network or information systems shall not be left unattended.

4.5.4   Every password shall be a combination of alphanumeric and be changed at regular intervals.

4.5.5   Departmental directories can be accessed by members of the department. The user's local directory on the PC can be accessed by only by the user.

4.5.6   Users must be made responsible for backing up files on their individual PC hard Drives as well as in the folder(s) in the server assigned by the Network Administrator (NWA), and departmental supervisors shall verify that users are doing so on a regular basis.

4.5.7   User shall be made responsible for the security of their individual workstations, including security of PC Backup disks.

4.5.8   Users shall also be made responsible for access security. Password shall not be written down or seen by others when they are keyed in. Other related responsibilities must include noting and reporting maintenance problems (such as disk error messages) before they can cause loss of data. Ensuing that the PC data disks are not subjected to excessive heat, electrical fields, dirt, smoke, food particles or spilled liquids: and also ensuring that the PC has a surge protector.

4.5.9   Users be made responsible for taking reasonable care of the system and reporting to a supervisor any maintenance problems, particular disks errors or other problems that might cause loss of data. Users will not remove / replace/ transfer/ hardware from ICB or to other locations within ICB without supervisory approval. Users shall avoid subjecting PCs to excessive vibration or bumps, hard jolts while a PC is running can damage a hard disk drive. Smoke, heat, magnetic fields and excessive dust can also damage LAN equipment. Each PC shall have a surge protection. Users will have to use good judgment when eating or drinking in the vicinity of PCs and LAN equipment.

4.5.10   All network users be made responsible for being familiar with the network operating and security procedures.

4.5.11   Warning messages will have to be carefully evaluated by the users and corrective actions will have to be taken timely.

4.5.12   screen saver (with in resume, display log on screen) to be used to protect desktop and laptop from unauthorized access.

4.5.13   Automatic screen saver be activated after a period of not more than five (5) minutes of inactivity.

4.5.14   Laptop Computers, computer media and any other forms of removable storage (e.g. diskettes, CD-ROMs, Flash Drives) will be stored in a secured location or locked cabinet, when not in use.

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

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

4.5.17 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.)

4.5.18 Any kind of viruses shall be reported immediately.

4.5.19 Viruses shall not be deleted without expert assistance unless otherwise instructed.

4.6   Personal Use of Network Resources / Databases/ Servers

4.6.1 Employees of ICB are prohibited from using ICB's Network /Database/Servers for personal work without the written approval of competent authority.

4.6.2 Network /Database/Servers access shall be restricted to normal working hours.

4.6.3 DBA may grant exceptions based on excess time need if required by departmental head.

4.6.4 Adequate supervisory and review of work be ensured for users who have access beyond normal working hours.

4.7   Restriction on Software Ownership & Authorization

4.7.1 All software installed on ICB's PCs and on the network shall comply with the Software's Licensing Agreement(s).

4.7.2 Server will be limited to the number of users covered by the license.

4.7.3 An original disk / CD must exist for each commercial software application installed on a user's PC.

4.7.4 Any unauthorized software shall not be installed on ICB's computers and devices.

4.7.5 Only software authorized by the proper authority shall be installed on a network or an individual's PC.

4.7.6 Users shall not install personal software on a PC without the approval of the proper authority.

4.7.7 Game(s) or entertainment package(s) must not be installed on any PC or network by any user.

4.7.8 The use of other than standard authorized software must be discouraged.

4.7.9 The list of authorized software shall be published by the ICT wing.

4.7.10 Users MUST NOT copy any purchased/ICB-developed/ICB-Owned Software for their personal use or distribution or any other purpose. ICB Software may be copied only for legitimate backup purposes.

4.7.11 PC software developed by ICB's employee(s) on ICB- owned equipment and/ or during normal working hours will be owned by the ICB.

4.7.12 ICT wing shall have to maintain an inventory of the software, software documents, licenses and copyright etc.

Chapter 5
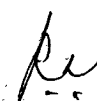
5. ICT Risk Management

ICT risk is a component of the overall risk universe of an enterprise. Other risks ICB 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 ICB. 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.

5.1 ICT Risk Governance

5.1.1 Risk Management Committee shall be formed to govern overall ICT risks and relevant mitigation measures.

5.1.2 Risk Appetite (amount of risk ICB is prepared to accept to achieve its' objectives) shall be defined in terms of combinations of frequency and magnitude of a risk to absorb loss e.g., financial loss, reputation damage.

5.1.3 The Risk Tolerance shall be defined (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.

5.1.4 Risk appetite and tolerance shall be reviewed and approved and shall be changed 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.

5.1.5 The risk responsibilities to individuals shall be defined for ensuring successful completion.

5.1.6 The risk accountability shall be defined that 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.

5.1.7 All risks by Risk Awareness shall be acknowledged so that those are well understood and known and recognized as the means to manage them.

5.1.8 Executive management's understanding of the actual exposure to ICT risk shall be contributed by Open Communication, enabling definition of appropriate and informed risk responses.

5.1.9 All internal stakeholders shall be aware of the importance of integrating risk and opportunity in their daily duties.

5.1.10 The actual level of risk and risk management processes in use shall be transparent to external stakeholders.

5.1.11 Risk-aware Culture shall be established from the top with board and executives, who set direction, communicate risk-aware decision making and reward effective risk management behaviors.

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

5.2 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.

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

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

5.2.1 Business impact analysis shall be established to understand the effects of adverse events. Several techniques and options might be practiced that can help to describe ICT risks in business terms.

5.2.2 The development and use of Risk Scenarios technique shall be practiced 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.

5.2.3 Risk Factors shall be defined those influence the frequency and/or business impact of risk scenarios.

5.2.4 Risk factors shall be interpreted as casual factors of the scenario that is materializing, or as vulnerabilities or weaknesses.

5.2.5 Periodic ICT risk assessment of ICT related assets (Information, process and systems) shall be conducted and recommendation to risk owners for mitigation shall be provided.

5.3 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.

5.3.1 A set of metrics shall be developed to serve as risk indicators. Indicators for risks with high business impact are most likely to be Key Risk Indicators (KRIs).

5.3.2 Effort shall be given to implement measure and report different indicators that are equivalent in sensitivity.

5.3.3 Selection of the right set of Key Risk Indicators (KRIs), ICB shall carry out:

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

    5.3.3.2 Provide a backward-looking view on risk events that have occurred

    5.3.3.3 Enable the documentation and analysis of trends

    5.3.3.4 Provide an indication of the risk's appetite and tolerance through metric setting

    5.3.3.5 Increase the likelihood of achieving the strategic objectives

    5.3.3.6 Assist in continually optimizing the risk governance and management environment

5.3.4 Risk response shall be defined to bring risk in line with the defined risk appetite for ICB after risk analysis.

5.3.5 Overall ICT risk management practices shall be strengthened with sufficient risk management processes.

5.3.6 A number of control measures shall be introduced intended to reduce either of an adverse event and/or the business impact of an event.

5.3.7 Risk frequency or impact shall be shared or reduced by transferring or otherwise sharing a portion of the risk, e.g. insurance, outsourcing.

Chapter 6

6. Business Continuity and Disaster Recovery Management

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

6.1   Business Continuity Plan (BCP)

6.1.1   There must be an approved Business Continuity Plan addressing the recovery from disaster to continue its operation.

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

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

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

6.1.5   BCP shall address the followings:

    6.1.5.1   Action plan to restore business operations within the specified time frame for: A) office hour disaster B) outside office hour disaster.

    6.1.5.2   Emergency contacts, addresses and phone numbers of employees, venders and agencies.

    6.1.5.3   Grab list of items such as backup tapes, laptops, flash drives, etc.

    6.1.5.4   Disaster recovery site map

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

6.2   Disaster Recovery Plan (DRP)

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

A Disaster Recovery Site (DRS) shall be established which is geographically separated from the primary site (minimum of 10 kilometers radial distance but choice of different seismic zone will

be preferred) to enable the restoration of critical systems and resumption of business operations when a disruption occurs at the primary site.

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

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

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

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

6.2.5 Inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests shall be considered.

6.2.6 Recovery strategies and technologies shall be explored such as on-site redundancy and real-time data replication to enhance the ICB's recovery capability.

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

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

6.2.9 The effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures shall be tested and validated at least annually.

6.2.10 Business users shall be involved in the design and execution of comprehensive test cases to verify that recovered systems function properly.

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

6.3 Data Backup and Restore Management

6.3.1 A data backup and recovery policy shall be developed. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off-line backups and the transfer of backups to secure off-site storage.

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

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

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

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

6.3.6 The backup inventory and log sheet (**Annexure -10: Back Up Log Book**) shall be maintained, checked and signed by the supervisor/ Branch Manager/ Head of the Department/Office.

6.3.7   Backup data shall be encrypted in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.

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

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

6.3.10 Periodic testing and validation of the recovery capability of backup media shall be carried out and assess whether it is adequate and sufficiently effective to support the ICB's recovery process.

6.4   Backup and Restoration Model

The following Data Backup and Restoration model will be followed until further development of any model by the ICT Wing:

6.4.1   The main server and the backup server will have the same configuration in order to keep the system running without any halt;

6.4.2   A computer will be kept for mirroring data from the main server;

6.4.3   The backup time and the backup procedure will be set. A particular time has to be reserved for taking backup;

6.4.4   Everyday incremental / cumulative backup of files and database will be taken;

6.4.5   No full-system backup will be done at the end of day. Full system backup and complete database backup will be taken at the end of every week;

6.4.6   Archiving will be done monthly;

6.4.7   Data backup will be kept in hard drive(s), CDs and tape drives. Off-site data backup procedure will be adopted;

6.4.8   If necessary, third party software will be used for taking data backup;

6.4.9   The responsibility of taking data backup(s) will be taken by a Data Backup Manager or NWA or DBA as the case may be;

6.4.10 The responsibility of restoring data will be performed by NWA / DBA;

6.4.11 Backup of system state data will be taken at regular intervals;

6.4.12 Every user will backup data locally and then save data in a particular folder in the server. The Administrator will subsequently backup all user data and the system data centrally to the backup server as well as removable storage devices;

6.4.13 The network administrator will identify critical and / or sensitive network data files and applications and ensure that these are adequately protected and backed up;

6.4.14 The NWA / DBA will be responsible for taking backup at the Head Office of ICB. The responsibility for backing up at Branches will lie with the officer(s) responsible for taking backup. Every user will backup data locally and then save data in a particular folder in the server. The System Administrator will subsequently backup all user data and the system data from the server to appropriate storage devices;

6.4.15 On-site backup tapes will be kept in a location sufficiently remote from the server. Specifically, the most current tape of a five-day rotation of backup tapes will be kept in a fireproof cabinet at the Head office, and the remaining four tapes to be stored in a fireproof cabinet at off building Branches;

6.4.16 There will be at least one backup copy kept on-site for time critical delivery;

6.4.17 There will be a folder in the name of each Department / Office in the server;

6.4.18 There will be a sub-folder for each subject under the main folder assigned for each Department / Office;

6.4.19 Data Backup Schedule:

Sunday to Wednesday   --------   backing up changed files

| Thursday | -------- | backing up all files |
| End of every month | -------- | archiving from backup copies |

6.4.20 For quick data backup, a combination of normal and differential backups will be adopted;

6.4.21 Clear documentation will be maintained for each backup. After each backup, a log has to be taken in printed form and signed by authorized person(s);

6.4.22 Data Restoration:

    6.4.22.1 The restoration procedure will be determined on the basis of type(s) of data backup;

    6.4.22.2 At regular intervals, data restoration procedure will be carried out on trial basis in order to check the workability of the backup media and backup wizard;

6.4.23 Data Archiving

    6.4.23.1 The directories and files / database data required for archiving will have to be determined;

    6.4.23.2 Whether particular files and folders will be stored in the server must be determined;

    6.4.23.3 The archiving procedure be executed;

    6.4.23.4 The files and / or folders / database data those are no longer required from the server will be removed at regular basis;

    6.4.23.5 Hard copies of data archive will have to be properly preserved; and

    6.4.23.6 The media in which files have been archived be stored in a safe place.

6.4.24 Data Recovery:

    6.4.24.1 NWA / DBA will be assigned with the responsibility of recovering data from proper backups;

    6.4.24.2 Data will be recovered from Hot Backups / Cold Backup in case of media failure;

    6.4.24.3 Data will be restored to a new disk(s) basing on parity information in other disk(s) in case of disk crash;

    6.4.24.4 The system will be put back to its operation from the backup server in case the main server fails to operate;

    6.4.24.5 Data will be recovered from the logical backup files, if full database is lost.

6.4.25 Disaster Management:

    6.4.25.1 The System Administrator (NWA / DBA) be proactive. He / She will take proper measures before any disaster occurs;

    6.4.25.2 All data will be backed up as per backup schedule;

    6.4.25.3 The whole system will be scanned at regular intervals for keeping the system virus free;

    6.4.25.4 The System Administrator will ascertain if alternative site for disaster recovery technology and applications are in place;

    6.4.25.5 The System Administrator will make the DR site well equipped with compatible hardware and telecommunication equipment to support the live systems in the event of a disaster;

    6.4.25.6 A logical security will be maintained throughout the fallback and DR process;

    6.4.25.7 An up-to-date and tested copy of the DR plan will have to be prepared and kept off-site;

    6.4.25.8 A DR test (rehearsal) be carried out successfully every three months;

    6.4.25.9 DR test documentation will include at a minimum the scope of planned tests, expected success criteria, plan with timetables and test results;

    6.4.25.10 The System Administrator / NWA / DBA will prepare and design a Contingency Plan. A plan for LAN Hardware and Software Recovery of critical network applications and data files will be included in the Contingency Plan of ICB.

Chapter 7

7. Acquisition and Development of Information Systems

For any new application of business function for ICB 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. System deficiencies and defects shall be identified at the system design, development and testing phases. Project Management approach shall be exercised for accusation and development of Information Systems. A steering committee shall be established for any project, 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.

7.1   ICT Project Management

Project management is the practice of initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time. ICT project management involves a structured approach to planning, organizing, leading, and controlling information and communication technology projects. There are various types of ICT including Software development and implementation, Software upgrades, Hardware installations and upgrades, Network system installations and upgrades, Data management, Data Migration, cloud computing and virtualization rollouts, business analytics and data management, implementing ICT services etc.

7.1.1   In drawing up a project management framework, it shall be ensured 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 roles and responsibilities of staff involved in the project shall be clearly defined in the project management framework.

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

7.1.3   It shall be ensured 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.

7.1.4   Management oversight of the project shall be established to ensure that milestones are reached and deliverables are realized in a timely manner.
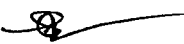
7.2 Vendor Selection for System Acquisition

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

7.2.2 Vendor selection process must have conformity with the Procurement Policy of the ICB.

7.2.3 Vendor selection criteria for application must address followings:

- 7.2.3.1 Market presence
- 7.2.3.2 Years in operation
- 7.2.3.3 Technology alliances
- 7.2.3.4 Extent of customization and work around solutions
- 7.2.3.5 Financial strength
- 7.2.3.6 Performance and Scalability
- 7.2.3.7 Number of installations
- 7.2.3.8 Existing customer reference
- 7.2.3.9 Support arrangement
- 7.2.3.10 Local support arrangement for foreign vendors
- 7.2.3.11 Weight of financial and technical proposal

7.3 In-house Software Development

7.3.1. Secure programming methods and testing are used for application development in order to minimize the number of coding errors and security vulnerabilities.

7.3.2. Software development shall follow recognized standard good practice including Requirement Analysis, Requirement approval, System Design, Coding, Testing, Documentation, Security Planning, Auditing, Certification and Accreditation.

7.3.3. Software development must segregate development, testing and production environments to limit the spread of malicious code and minimize the likelihood of faulty code being put into production. It must be ensured that software development environments are configured such that:

a) There are at least three separate environments with separate personnel covering:

    I. Development
    II. Testing
    III. Production

It is better to have more separately segregated units in software development process such as System analysis and design, Project Management, Documentation, Change Management, Research and Training etc.

b) Information flow between the environments must be strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement.

c) New development and modifications must only take place in the development environment.

d) Write access to the authoritative source for the software (source libraries & production environment) shall be disabled.

e) ICT Security, ICT audit and ICT compliance recommendation must be considered while designing and coding any in house software.

7.3.4. ICB shall ensure that software developers use secure programming practices when writing code, including:

a) designing software to use the lowest privilege level needed to achieve its task

b) denying access by default

c) checking return values of all system calls

d) validating all inputs

7.3.5. Software development activities and all the in-house developed software must undergo Certification and Accreditation process.

7.3.6. Detailed business requirements shall be documented and approved.

7.3.7. Detailed technical system design shall be prepared and approved.

7.3.8. Application security and availability requirements shall be addressed and shall be approved.

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

7.3.10. In-house software development shall follow standardized software development procedure. Adequate technical personnel shall be employed to maintain standardized procedures in software development.

7.3.11. Industry standard certification shall be obtained related to software development environment, procedures and management.

7.3.12. Appropriate project management approach shall be established for in-house software development.

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

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

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

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

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

7.3.18. Application shall be in compliance with relevant controls of ICB's ICT Security Policy.

7.3.19. Necessary 'Regulatory Compliance' requirements must be taken into account by ICB.

7.3.20. Software systems must have proper accreditation before it is used in a production environment.

7.3.21. Software shall be reviewed or tested for vulnerabilities before it is used in the production environment. Proper VA/PT must be performed for all the in house developed software and measures shall be taken accordingly to address relative security risks before used in the production environment.

7.3.22. Software shall be reviewed or tested by developer-independent testers/quality assurers as well as the developers.

7.3.23. Software development shall follow secure coding practices.

7.3.24. For any transaction entry, there must be at least two individuals necessary for its completion. The one who makes the transaction entry (i.e. maker) cannot be the same one who checks (i.e. checker) it.

7.3.25. A transaction entry is only considered completed if it has been checked.

7.3.26. Software reviewing and testing will reduce the possibility of introducing vulnerabilities into a production environment.

7.3.27. Only authorized software and tools shall be used for Software development. Authorized Software/ Platform/ Languages/ tools used in in-house software development shall be procured/collected in a proper way.

7.4 Software Documentation

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

7.4.2 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

7.5 Statutory Requirements

7.5.1 All the software procured and installed by ICB, shall have legal licenses and record of the same shall be maintained by the respective unit/department of ICB.

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

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

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

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

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

7.6 Other Requirements

7.6.1 There shall have a test environment to ensure the software functionalities before implementation.

7.6.2 User Acceptance Test shall be carried out and signed-off before going live.

7.6.3 Necessary 'Regulatory Compliance' requirements for internet trading and banking procedures and practices in the application must be taken into account by ICB.

7.6.4 Any bugs and/or errors found due to design flaws, must not be escalated to higher levels in Software Vendors' organization and ICB, and must be addressed in time.

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

Chapter 8

8.   System Certification, Accreditation and Documentation

Certification and Accreditation is a fundamental governance and assurance process, designed to provide the Board of Directors, Managing Directors and senior management confidence that information and its associated technology are well-managed, that risks are properly identified and mitigated and that governance responsibilities can demonstrably be met. It is essential for credible and effective information assurance governance.

C&A has two important stages where certification must be completed before accreditation can take place. It is based on an assessment of risk, the application of controls described in the GOBISM and determination of any residual risk.

Certification and Accreditation are separate and distinct elements, demonstrate segregation of duties and assist in managing any potential conflicts of interest. These are important attributes in good governance systems.

There are four groups of participants in C&A process:

A.   System Owners, responsible for the design, development, system documentation and system maintenance, including any requests for recertification or reaccreditation

B.   The Certification Authority, responsible for the review of information and documentation provided by the system owner to ensure the ICT system complies with minimum standards and the agreed design

C.   The Assessor or Auditor, who will conduct inspections, audits and review as instructed by the Certification Authority

D.   The Accreditation Authority who will consider the recommendation of the Certification Authority, determine the acceptable level of residual risk and issue the system accreditation, the authority to operate a system.

8.1   The Certification and Accreditation Process

Certification is the assertion that an ICT system complies with the minimum standards and controls described in the policy, any relevant legislation and regulation and other relevant standards. It is based on a comprehensive evaluation or systems audit. The Certification Authority for ICB shall be delegated by the Managing Director.

Accreditation is the formal authority to operate a system, evidence that governance requirements have been addressed and that the management has fulfilled the requirement to manage risk on behalf of the organization and stakeholders. The Accreditation Authority for ICB is the Managing Director or their delegate (Member of senior management or CISO).

8.2   Conducting Certifications

8.2.1   All systems must undergo an audit as part of the certification process

8.2.2   The certification authority must accept that the controls are appropriate, effective and comply with the relevant components from ICB's ICT Security policy, GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL (GOBISM) and The Guideline on ICT Security for Banks and Non-Bank Financial Institutions published by Bangladesh Bank, in order to award certification.

8.2.3   Following the audit, the certification authority shall produce an assessment for the Accreditation Authority outlining the residual security risks relating to the operation of the system and a recommendation on whether to award accreditation or not

8.2.4   The Certification Authority for ICB shall be delegated by the Managing Director.

certification acknowledges only that controls were appropriate, properly implemented and are operating effectively. Certification does not imply that the residual security risk is acceptable or an approval to operate has been granted. The purpose of the residual security risk assessment is to assess the risks, controls and residual security risk relating to the operation of a system. In situations where the system is nonconformant, the system owner may have to take corrective actions. The residual risk may not be great enough to preclude a certification authority recommending to the Accreditation Authority that accreditation be awarded but the risk must be acknowledged and appropriate caveats documented.

System Certification and Accreditation Block Diagram
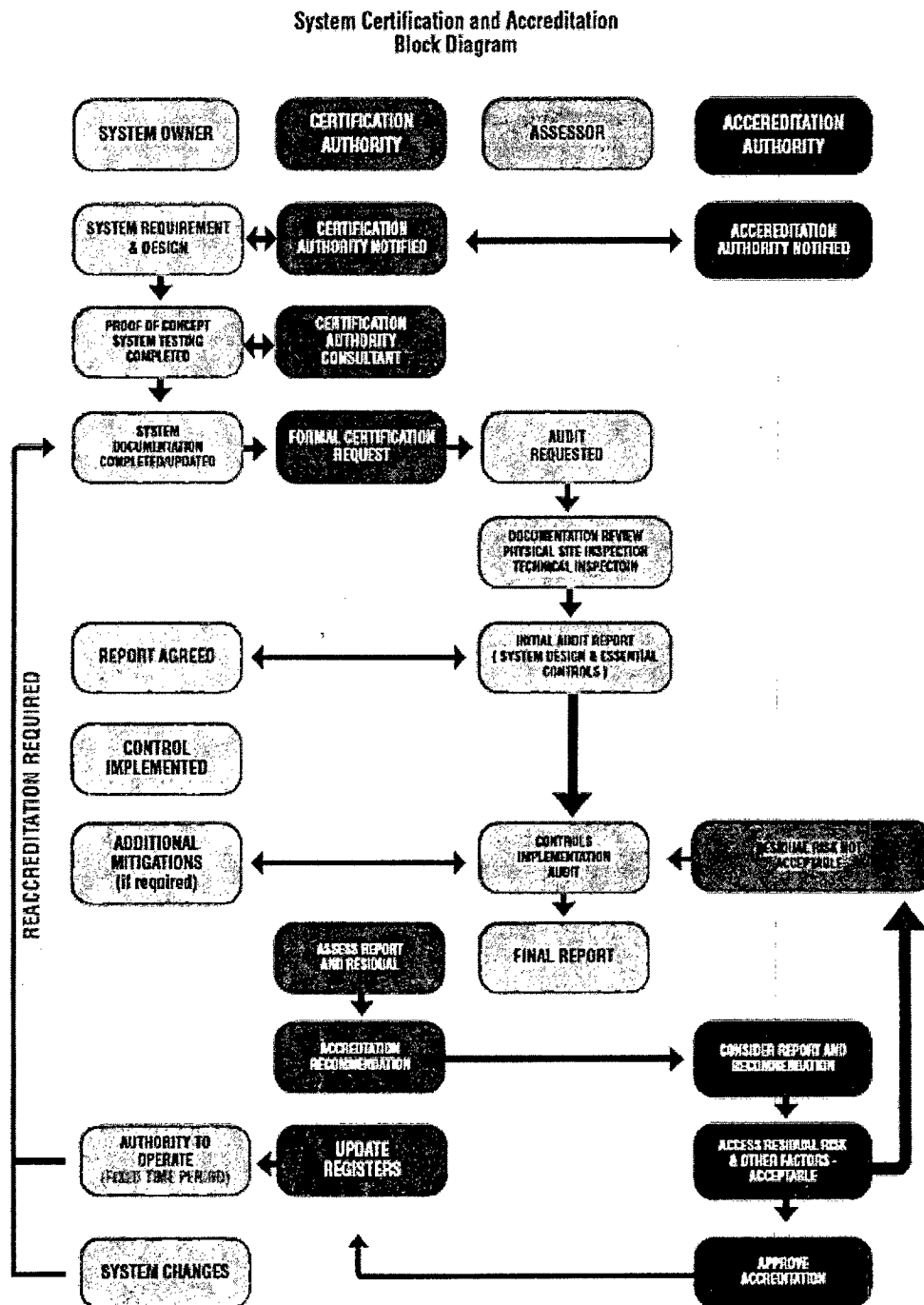
Figure 01: System Certification and Accreditation Block Diagram

8.3   Conducting Audits

8.3.1   The Information Security Policies, Security Risk Management Plans, System Security Plans, Standard Operating Procedures (SOP) and Incidence Response Plan (IRP) documentation must be reviewed by the auditor to ensure that it is comprehensive and appropriate for the environment the system is to operate within.

8.3.2   The Information Security Policy (SecPol) must be reviewed by the auditor to ensure that all relevant controls specified in this manual are addressed.

8.3.3   Prior to undertaking any system testing in support of the certification process, the system owner must implement the controls for the system.

8.3.4   The implementation of controls must be assessed to determine whether they have been implemented correctly and are operating effectively.

8.3.5   The auditor must produce a report of compliance for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

8.3.6   ICB shall ensure that auditors conducting audits are able to demonstrate independence and are not also the system owner or certification authority.

8.3.7   The system and security architectures shall be reviewed by the auditor to ensure that it is based on sound information security principles and meets information security requirements.

The aim of an audit is to review and assess:
- the risk identification
- design (including the system and security architectures)
- controls selection
- actual implementation and effectiveness of controls for a system
- supporting information security documentation.

The outcome of an audit is a report of compliance and control effectiveness for the certification authority outlining areas of non-compliance for a system and any suggested remediation actions.

An audit may be conducted by agency auditors or an independent security organization.

8.4   Accreditation Framework

8.4.1   An accreditation framework shall be developed for ICB's I CT systems.

8.4.2   All of the ICB's ICT systems must be awarded accreditation before they are used operationally.

8.4.3   All of the ICB's ICT systems must be awarded accreditation prior to connecting them to any other internal or external system.

8.4.4   It shall be ensured that the period between accreditations of each of their systems does not exceed three years

8.4.5   Any ICT system must not be operated without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation

8.4.6   It shall be ensured that information security monitoring, logging and auditing is conducted on all accredited systems

The development of an accreditation framework within ICB will ensure that accreditation activities are conducted in a repeatable and consistent manner. ICB shall reaccredit its ICT systems at least every two years. Accreditations shall be commenced at least six months before due date to allow sufficient time for the certification and accreditations processes to be completed. Once three years has elapsed between accreditations, the authority to operate the system (the accreditation) will lapse and ICB will need to either reaccredit the system or request a dispensation to operate without accreditation. It shall be noted that operating a system without accreditation is considered extremely risky.

8.5 Conducting Accreditations

As a governance good practice, systems are accredited before they are used operationally.

8.5.1 All systems must be certified as part of the accreditation process.

8.5.2 The Accreditation Authority must accept the residual security risk relating to the operation of a system in order to award accreditation. The aim of accreditation is to give formal recognition and acceptance of the residual security risk to a system and information it processes, stores or communicates.

8.5.3 The outcome of accreditation is an approval to operate issued by the Accreditation Authority to the system owner.

8.5.4 For ICBs the Accreditation Authority is the Managing Director as agency head or their delegate. Depending on the circumstances and practices of an agency, the Managing Director could choose to delegate their authority to multiple senior executives who have the authority to accept security risks for the specific business functions within ICB.

8.6 Information Security Documentation

8.6.1 ICB's ICT wing shall have a well-documented organogram for ensuring secured and state of the art ICT Operations.

8.6.2 ICT support unit/section/personnel shall be placed in the branch organogram with well-documented job descriptions for ICT personnel in the branches.

8.6.3 Each individual within ICT organogram (e.g. department/division/unit/branche) shall have approved Job Description (JD) with fallback resource person.

8.6.4 Segregation of duties for ICT tasks shall be maintained.

8.6.5 Detailed design document for all ICT critical software/systems/services (e.g. Software development, Data Center design, Network design, Power Layout for Data Center etc.) shall be maintained.

8.6.6 Prescheduled roster for sensitive ICT tasks (e.g. EOD operation, Network Monitoring, Security Guard for Data Center etc.) shall be maintained.

8.6.7 Updated Standard Operating Procedure (SOP) for all ICT functional activities (e.g. Software Development, Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery etc.) shall be maintained.

8.6.8 Approved relevant requisition/acknowledgement forms for different ICT request/development/operation/services shall be maintained.

8.6.9 There shall be User Manuals of all applications for internal/ external users.

8.6.10. There must have a Security Policy (SecPol). The SecPol is usually sponsored by the Managing Director and managed by the CISO or Chief Information Officer (CIO). The ITSM shall be the custodian of the SecPol.

8.6.11 It must be ensured that every system is covered by a Security Risk Management Plan (SRMP).

8.6.12 It must be ensured that every system is covered by a Security Plan (SecPlan) .

8.6.13 It must be ensured that Standard Operating Procedures (SOPs) are developed for ICT systems.

8.6.14 An Incident Response Plan (IRP) and supporting procedures must be developed.

8.6.15 ICB personnel must be trained in, and exercise the Incident Response Plan.

8.6.16 It must be ensured that their SecPol, SRMP, SecPlan, SOPs and IRP are appropriately classified.

8.6.17 ICB shall create and maintain an overarching document describing the ICB's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.

8.6.18 It must be ensured that SRMP, SecPlan, SOPs and IRP are logically connected and consistent for each system and with ICB's SecPol.

8.6.19 All information security documentation shall be formally approved and signed off by a person with an appropriate level of seniority and authority.

8.6.20 It must be ensured that all high-level information security documentation is approved by the CISO and the Managing Director or their delegates.

8.6.21 It must be ensured that all system-specific documents are reviewed by the ITSM and approved by the system owner.

8.6.22 A regular schedule shall be developed for reviewing all information security documentation.

Chapter 9

9. Alternative Delivery Channels (ADC) Security Management

Alternate Delivery Channels are methods for providing Financial services directly to the customers. Customers can perform transactions through their ATM, contact the 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 financial institutes 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   Online Transaction

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

9.1.1   Assurance shall be provided to customers and users so that online access and transactions performed over the internet are adequately protected and authenticated.

9.1.2   Security requirements shall be properly evaluated associated with online transaction system and adopt mechanisms which are well-established international standards.

9.1.3   Internet Banking/Online Transaction Security policy shall be formulated, considering technology security aspects as well as operational issues.

9.1.4   It shall be ensured that information processed, stored or transmitted between ICB and its customers is accurate, reliable and complete. Appropriate processing and transmission controls shall also be implemented to protect the integrity of systems and data, e.g. SSL, TLS.

9.1.5   2-FA (two-factor authentication) shall be implemented for all types of online financial transactions. Hardware/Software based tokenization means will be preferred. The primary objectives of two-factor authentication are to secure the customer authentication process and to protect the integrity of customer's financial transaction details as well as to enhance confidence in online systems.

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

9.1.7   Monitoring or surveillance systems shall be implemented to follow-up and address subsequently any abnormal system activities, transmission errors or unusual online transactions.

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

9.1.9   High resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment) shall be maintained. ICT Security Division/Department/unit shall put in place measures to plan and track capacity utilization

as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack).

9.1.10 ICT Security Division/Department/unit shall take appropriate measures to minimize exposure to other forms of attacks such as middleman. attack which is commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack.

9.1.11 ICT Security Division/Department/unit shall undertake periodic penetration tests of the system, which may include:

a) Attempting to guess passwords using password-cracking tools

b) Searching for back door traps in the programs

c) Attempting to overload the system using DDoS (Distributed Denial of Service) and DoS (Denial of Service) attacks

d) Checking middleman attacks

e) Checking of commonly known holes in the software, especially the browser and the e-mail software exist

f) Checking the weaknesses of the infrastructure

g) Taking control of ports

h) Cause application crash

i) Injecting malicious codes to application and database servers

9.1.12 Customers shall be educated on security measures to protect them in an online environment.

9.2 Mobile Financial Services

Controls over mobile transactions are required to manage the risks of working in an unprotected environment. Security controls, system availability and recovery capabilities shall be formulated which commensurate with the level of risk exposure, for operations.

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

9.2.2 Risks associated with the types of services being offered in the risk management process shall be clearly identified.

9.2.3 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.

9.2.4 An agreement shall be arranged 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.

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

9.2.6 Periodic risk management analysis and security assessment of the MFS operation shall be conducted and take appropriate measures accordingly.

9.2.7 There shall have conformity with 'Regulatory Compliance' requirements of the country.

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

Chapter 10

10. Service Provider Management

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

10.1 Outsourcing

Agreements of 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 It shall be ensured 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 ICB's internal controls. The service providers are required 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 service providers are required 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 security policies, procedures and controls of the service provider shall be monitored and reviewed 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 service providers are required 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 A contingency plan shall be developed 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 A service catalogue shall be maintained 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 Official authorization/assurance shall be provided 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 (SLA)

10.3.1 There shall have Service Level Agreements(SLA) between ICB 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 It shall be ensured that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

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

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

    a) Pricing

    b) Measurable service/deliverables

    c) Timing/schedules

    d) Confidentiality clause

    e) Contact person names (on daily operations and relationship levels)

    f) Roles and responsibilities of contracting parties including an escalation matrix

    g) Renewal period

    h) Modification clause

    i) Frequency of service reporting

    j) Termination clause

    k) Penalty clause

    l) Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies

    m) Geographical locations covered

    n) Ownership of hardware and software

    o) Documentation (e.g. logs of changes, records of reviewing event logs)

    p) Right to have information system audit conducted (internal or external).

Chapter 11

11. 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.

11.1 Change Management

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

11.1.2 ICT Change Management department/unit/team shall be established to govern and manage overall crucial changes in ICB's ICT system.

11.1.3 Business Requirement Document (BRD) shall be prepared which will cover the requirements of system changes and the impact that will have on business processes, security matrix, reporting, interfaces, etc.

11.1.4 All changes of business application implemented in the production environment must be governed by a formal documented process with necessary change details. A sample form has been provided in **Annexure- 2: Change Request Form.**

11.1.5 Audit trails shall be maintained for business applications.

11.1.6 Rollback plan shall be prepared for unexpected situation.

11.1.7 User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment. A sample form has been provided in **Annexure- 3: User Acceptance Test.** This document shall be prepared for ready reference.

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

11.2 Incident Management

An incident occurs when there is an unexpected disruption to the standard delivery of ICT services. Such incidents shall be managed appropriately to avoid a situation of mishandling that result in a prolonged disruption of ICT services.

11.2.1 An incident management framework shall be established with the objective of restoring normal ICT service as quickly as possible following the incident with minimal impact to the business operations. Roles and responsibilities of staff involved in the incident management process shall be established, which includes recording, analyzing, remediating and monitoring incidents.

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

11.2.3 Corresponding escalation and resolution procedures shall be established where the resolution timeframe is proportionate with the severity level of the incident.

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

11.2.5 An ICT Emergency Response Team shall be formed, comprising staff within ICB with necessary technical and operational skills to handle major incidents.

11.2.6 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. ICB shall inform Bangladesh Bank as soon as possible in the event that a critical system has failed over to its disaster recovery system.

11.2.7 Customers shall be 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 ICB.

11.2.8 As incidents may trail from numerous factors, a root-cause and impact analysis shall be performed for major incidents which result in severe disruption of ICT services. Remediation actions shall be taken to prevent the recurrence of similar incidents.

11.2.9 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.

11.2.10 Incidents shall be adequately addressed within corresponding resolution timeframes and monitor all incidents to their resolution.

11.3 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.

11.3.1 A process shall be established to log the information system related problems.

11.3.2 The process of workflow shall be there to escalate any problem to a concerned person to get a quick, effective and orderly response.

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

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

11.4   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, it shall be ensured that indicators such as performance, capacity and utilization are monitored and reviewed.

4.4.2   Monitoring processes shall be established and appropriate thresholds shall be implemented to plan and determine additional resources to meet operational and business requirements effectively.

11.5   Standard Operating Procedures (SOPs)

Standard Operating Procedures (SOPs) ensure security procedures are followed in an appropriate and repeatable manner. SOPs provide step-by-step guides to undertaking information security related tasks and processes. They provide assurance that tasks can be undertaken in a secure and repeatable manner, even by system users without strong technical knowledge of the system's mechanics. In order to ensure that personnel undertake their duties in an appropriate manner, with a minimum of confusion, it is important that the roles of ITSMs, administrators, developers and system users are covered by SOPs.

11.5.1 Operating procedures must exist for all ICT systems.

11.5.2 Changes to operating procedures will be authorized by management and always be documented.

11.5.3 Operating procedures shall cover the followings where appropriate:

   a) Documentation on handling of different processes;

   b) Scheduling processes (including target starts and finish times);

   c) Documentation on handling of error and exception conditions;

   d) Documentation for secure disposal of output from failed processing runs;

   e) Documentation on system start-up, shut -down, restart and recovery;

   f) Schedule system maintenance.

11.5.4 The roles of ITSMs, administrators, developers and system users shall be covered by SOPs.

11.5.5 ITSMs, system administrators and system users shall sign a statement that they have read and agree to abide by their respective SOPs.

11.6   Recording Request / Maintenance History

For ready reference, a file / register will have to be opened for recording history relating to troubleshooting so that problem(s) can be solved easily in future.

Chapter 12

12. Customer Education

With the advent of online services, customer's experience of getting services is therefore no longer fully under control of ICB. 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 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.

12.1 Awareness Program

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

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

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

12.1.3 Proper contents shall be created and published.

12.1.4 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).

12.1.5 The right message content shall be delivered to the right audience using the most effective communication channels.

12.1.6 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) Recorded messages played during waiting period of phone banking calls

12.1.7   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)   Emails and SMS texts

     c)   Common website developed with content from all stakeholders

     d)   Groups, games and profiles on social media

     e)   Bill boards

     f)   Online training modules and demos hosted on this site

     g)   Posters in prominent locations such as petrol pumps, popular restaurants, shopping malls, etc.

     h)   Interactive guidance in the form of help lines

     i)   Customer meets and interactive sessions with specialists

     j)   Talk shows on television/radio

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

Chapter 13

13. Do's and Don'ts for Users

13.1 Do's

13.1.1 Every user must log off before leaving his/ her computer (Desktop/Laptop etc.):

13.1.2 Desktop computers, laptops, monitors, etc. shall be turned off (properly shutdown) at the end of each workday.

13.1.3 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.

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

13.1.5 Every password shall be a combination of uppercase letters, lowercase letters, numbers and special characters and shall be changed at regular intervals according to ICT security policy of ICB.

13.1.6 Users must be made responsible for backing up important, necessary, official files on their individual PC hard Drives as well as in the folder(s) in the server assigned by the Network Administrator (NWA), and departmental heads shall verify those users are doing so on a regular basis.

13.1.7 User shall be made responsible for any kind of illegal or unauthorized use of their individual workstations and security of official data.

13.1.8 Users be made responsible for taking reasonable care of the system and reporting to a supervisor any maintenance problems, particular disks errors or other problems that might cause loss of data. Users will not remove / replace/ transfer/ hardware from ICB or to other locations within ICB without prior approval.

13.1.9 All network users be made responsible for being familiar with the network operating and security procedures.

13.1.10 Warning messages will have to be carefully evaluated by the users and corrective actions will have to be taken timely.

13.1.11 Screen saver (with in resume, display log on screen) to be used to protect desktop and laptop from unauthorized access.

13.1.12 Internet shall be used according to the written approval of competent authority.

13.1.13 Any kind of viruses or unusual activities shall be reported immediately to the authority.

13.1.14 Email system shall be used according to the ICB's policy.

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

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

13.1.17 Email transmissions from ICB must have a disclaimer stating about confidentiality of the email content and asking intended recipient.

13.2 Don'ts

13.2.1 Employees of ICB are prohibited from using ICB's Network /Internet/Database/Servers for personal work without the written approval of competent authority.

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

13.2.3 Laptop computers actively connected to the network or information systems shall not be left unattended.

13.2.4 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.)

13.2.5 Password shall not be written down or seen by others when they are keyed in.

13.2.6 Users must not share their password with others or write them down. Users are responsible for all activities associated with their credentials.

13.2.7 Employees shall be prohibited from establishing their own connection to the Internet using ICB's systems or Devices.

13.2.8 Use of locally attached modems with ICBs' systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved and before disconnecting from LAN.

13.2.9 Users must not copy any purchased/ICB-developed/ICB-Owned Software, sensitive/important official documents/information for their personal use or distribution or any other purpose. ICB Software may be copied only for legitimate backup purposes.

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

13.2.11 Users must not click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.

13.2.12 Users must not open mail or attachments from an untrusted source. If user receive a suspicious email, the best thing to do is to delete the message, and report it to your manager and Information Security Officer (ISO)/designated security representative

13.2.13 Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of ICB, or contain any material that is harmful to employees, customers, competitors, or others.

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

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

Penalties and discipline

Employee who acts against this policy will face disciplinary action in accordance with the service regulation of ICB. Contractual service provider, temporary or part-time stuff also face disciplinary action including termination of service.

Policy, monitoring and review

Managing Director shall delegate the responsibility to a committee for the review of this policy. The committee shall ensure that:
• This policy is reviewed regularly, preferably at least once in a calendar year.
• Compliance with this policy is monitored/audited on a regular basis, as determined by risk assessment.
• Effectiveness of this policy shall be reported to Managing Director.

Conclusion

The increasing use of ICT has caused the integration of various economic units in a way that has made business operations to be highly ICT inclined and to benefit immensely from the gains in technological revolution. ICT is found to impact positively the speed of customer service delivery, as well as productivity and profitability. For this, ICB will train its Human Resources from time to time to keep them abreast of the innovations in the use of ICT. This ICT Security Policy will help to ensure quality service delivery and productivity of ICB. From now on the ability of ICB to retain its existing customers and attract prospective ones will be enhanced, which is mainly a function of its efficient service delivery that depends on the use of ICT.

Annexure: 1
Dispensation Form

Reference: Date:

Section I: Requester Information

Name of the Institution   :
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/Applicants/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

<u>Change Request Form</u>

Reference: **Date:**

Section I: Requester Information

Branch/Division Name   :

Submitted by   :

Change Description   :

Change Purpose   :

Request Date   :

Signature & Seal   Signature & Seal

(Requester)   (Head of Branch/Division)

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   :

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
Stock Register of Hardware and Software

Name of the item: --

Sl No	Brand & Model	Description with Specification/version	Quantity	ID NO	Machine Location	Supplier/ Vendor	Date of Supply	Price	Signature	remarks
01	02	03	04	05	06	07	08	09	10	11

Annexure: 5
Access Authorization List

Serial no	Name and designation of the authorized persons	address	Authorization validity		- Authorization card no.	Authorized by	remarks
			from	to			
01	02	03	04	05	06	07	08

Annexure: 6
Access Log Book
(for the use in the Data Center, Server Room, Computer Room)

Date of Access	Name and designation of the authorized persons	Address	Authorization card no	Time of Access	Signature of the Person	Purpose of access/ work done	Time of the Departure	Signature of the person	remarks
01	02	03	04	05	06	07	08	09	10

Annexure: 7
Visitors Log Book
(or the use in the Data Center, Server Room, Computer Room)

Date of visit	Name of the visitor	address	Purpose of visit	Time of Access	Signature of the visitor	Work done/ Activities during stay	Time of the Departure	Signature of the Authorized Person	remarks
01	02	03	04	05	06	07	08	09	10

Annexure: 8
User Creation Form

Reference: **Date:**

01.

Name of the user   :

Employee ID of user   :

Designation   :

Address   :

Date of joining   :

Transfer From   :

Contact No   :

02. Name of the System / Software:

03. User Status: Administrator/ Data Controller / Data Processor /Data Operator/Data Viewer/Others (Specify)

04. User Rights Propose: Module Name(s) and user right (Read, Write, Delete, Copy, Change etc.)

Signature & Seal   Signature & Seal
(User)   (Recommended / Proposed by)

Approved By....

Signature & Seal
(System Owner/System Manager/ Branch Manager/ Head of Department of Office)

(For the use of ICT Authority/ System owner/ Authorized Officer)
Accepted for implementation for the following rights:

1.   User Created :
2.   a) On : ----------------------------
3.   b) User ID : ---------------------
4.   c) User password Envelop No:
5.

Signature & Seal   Signature & Seal

(CISO/System Owner/System Manager/Branch Manager)   (Authorised Officer/In charge of System Administration)

Annexure: 9
Password Handover Form

Reference: **Date:**

      We, the undersigned handing over and receiving respectively today the............*(date)* at ....am/pm the sealed cover in respect of the followings:

(1)...

(2)...

(3)..in terms of the order

no...dated..............of ....

.... *(name of the order issuing office)* ....in presence of the following witness (officer/staff).

Signature:

(Handing over Officer) Name :

ID:

Designation:

Address :

Counter Signature:

Name of the counter signing officer:

ID:

Designation:

Address :

  B: *After receiving the passwords the receiving officer will open the sealed envelope alone and confirm the passwords applying in the system/database. S/he will change the passwords just after checking and again handed over the same in a sealed envelope to the Head of the Computer Department/branch manager documentarily.*

Annexure: 10
Back Up Log Book

Name of the System: ---

| SI No | Backup Period / Date | Backup Media | Backup Type (Full/ incremental) | Backup taken By | | | Back up send to | Ref./ Code No | Recipi ent | Remarks |
				Name and ID	Designation	Signature				
01	02	03	04	05	06	07	08	09	10	11

Annexure: 11
Handover/Takeover of ICT Asset

Reference: **Date:**

      We, the undersigned handing over and receiving respectively today the............(*date*) at ....am/pm respect of the followings:

(1)..

(2)..

(3)..

Signature:
(Handing over Officer) Name :
ID:
Designation:
Address :

Counter Signature:
Name of the counter signing officer:
ID:
Designation:
Address :

Witness:

Glossary and Acronyms

2FA   - Two-Factor Authentication
ADC   - Alternative Delivery Channel
AMC   - Annual Maintenance Contract
AML   - Anti-Money Laundering
ATM   - Automated Teller Machine
BCP   - Business Continuity Plan
BIA   - Business Impact Analysis
BRD   - Business Requirement Document.
BYOD   - Bring Your Own Device
CAAT   - Computer-Assisted-Auditing Tool
CCTV   - Close Circuit Television
CD ROM- Compact Disk Read Only Memory
CDs   - Compact Disks
CEO   - Chief Executive Officer
CIO   - Chief Information Officer
CISO   - Chief Information Security Officer
CNP   - Card Not Present
CTO   - Chief Technology Officer
DC   - Data Center
DDoS   - Distributed Denial of Service
DoS   - Denial of Service
DR   - Disaster Recovery
DRP   - Disaster Recovery Plan
DRS   - Disaster Recovery Site
DVD   - Digital Video Disc
E-mail   - Electronic Mail
EOD   - End of Day
GOBISM - GOVERNMENT OF BANGLADESH INFORMATION SECURITY MANUAL
ICC   - Internal Control and Compliance
ICT   - Information and Communication Technology
IDS   - Intrusion Detection System
IPS   - Intrusion Prevention System
IS   - Information System
ISDN   - Integrated Services Digital Network
ICB   - Investment Corporation of Bangladesh
ICT   - Information and Communication Technology
IVR   - Interactive Voice Response
JD   - Job Description
KRIs   - Key Risk Indicators
MITMA - Man-in-the-Middle Attack
NBFI   - Non-Bank Financial Institution
OTP   - One Time Password
PCI DSS- Payment Card Industry Data Security Standard
PCs   - Personal Computers
PDA   - Personal Digital Assistant
PIN   - Personal Identification Number

PODs   - Personally Owned Devices
POS   - Point of Sale
PSTN   - Public Switched Telephone Network
RPO   - Recovery Point Objective
RTO   - Recovery Time Objective
SDLC   - Software Development Life Cycle
SMS   - Short Messaging Service
SQL   - Structured Query Language
SSL   - Secured Socket Layer
TLS   - Transport Layer Security
TV   - Television
UAT   - User Acceptance Test
UPS   - Uninterrupted Power Supply
USB   - Universal Serial Bus
User ID - User Identification
UTP   - Unshielded Twisted Pair
VA   - Vulnerability assessment
VA/PT   - Vulnerability assessment and Penetration Testing
VLAN- Virtual Local Area Network
VPN   - Virtual Private Network
WAN   - Wide Area Network
WLAN   - Wireless Local Area Network

References:

1.   ICT Security policy and Guideline 2015, Version 1.0, Investment Corporation of Bangladesh(ICB)
2.   Guideline on ICT Security For Banks and Non-Bank Financial Institutions, May 2015, Version 3, Bangladesh Bank
3.   Government of Bangladesh Information Security Manual, version 1.5, 2016