

Guideline on ICT Security For Scheduled Banks and Financial Institutions

April, 2010
Version 2.0



Bangladesh Bank

Technical Team

Coordinator

Salima Khatun
Senior Systems Analyst
IT Operation & Communication Department
Bangladesh Bank

Members

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

Md. Raihan Uddin
Joint Director
Department of Banking Inspection-1
Bangladesh Bank

Manoj Kumar Howlader
Joint Director
Foreign Exchange Inspection & Vigilance Department
Bangladesh Bank

Jayanta Kumar Bhowmick
Programmer
IT Operation & Communication Department
Bangladesh Bank

Md. Lutful Haidar Pasha
Assistant Director
Banking Regulations and Policy Department
Bangladesh Bank

Muhammed Anwarul Islam
Senior Assistant Vice President & Head of IT Security
Eastern Bank Limited

Sk. Zaminur Rahman
Senior Systems Analyst
Information Technology System Department
Janata Bank Limited

ANM Kamrul Islam
Relationship Manager (IT)
Standard Chartered Bank

M. Asheq Rahman
Vice President
Head of Regulatory & Internal Control
BRAC Bank Limited

Md. Mashuqur Rahman
Senior Principal Officer
IT Division
AB Bank Limited

Contents

CHAPTER 1.....	1
1. Introduction.....	1
1.1 Scope	1
1.2 Objectives.....	2
1.3 Categorization of banks/branches/units depending on ICT Operation.....	2
CHAPTER 2.....	4
2. ICT Security Management	4
2.1 ICT Security Policy	4
2.2 Documentation.....	5
2.3 Internal Information System Audit	5
2.4 Training and Awareness	6
2.5 Insurance or Risk Coverage Fund	6
2.6 Problem Management.....	6
2.7 Risk Management.....	6
CHAPTER 3.....	8
3. ICT Operation Management	8
3.1 Change Management	8
3.2 Asset Management	8
3.3 Operating Procedures	9
3.4 Request Management	9
CHAPTER 4.....	10
4. Physical Security	10
4.1 Physical Security for Tier-1	10
4.1.1 Data Center Access	10
4.1.2 Environmental Security.....	11
4.1.3 Fire Prevention	12
4.2 Physical Security for Tier-2	13
4.2.1 Server Room Access.....	13
4.2.2 Environmental Security.....	13
4.2.3 Fire Protection	14
4.3 Physical Security for Tier-3	14
4.3.1 Computer Room Access	14
4.3.2 Environmental Security.....	14
4.3.3 Fire Protection	14
4.4 Physical Security for Desktop and Laptop Computers.....	15
CHAPTER 5.....	17
5. Information Security Standard	17
5.1 Access Control for Information Systems	17
5.1.1 User ID Maintenance	17
5.1.2 Password Control.....	17

5.1.3	Input Control	18
5.2	Network Security	18
5.3	Data Encryption	19
5.4	Virus Protection	19
5.5	Internet and e-mail	19
5.6	Transactions through Alternative Channels	20
5.6.1	Services through Mobile	20
5.6.2	Internet Banking	21
5.6.3	Payment Cards	22
 CHAPTER 6		 24
6.	Software Development and Acquisition	24
6.1	In-house Software	24
6.2	Outsourced Software	25
6.2.1	Vendor Selection	25
6.2.2	Software Documentation	25
6.2.3	Other Requirements	26
 CHAPTER 7		 27
7.	Business Continuity and Disaster Recovery Plan	27
7.1	Business Continuity Plan (BCP)	27
7.2	Disaster Recovery Plan (DRP)	28
7.3	Backup and Restore Plan (BRP)	28
 CHAPTER 8		 30
8.	Service Provider Management	30
8.1	Service Level Agreement (SLA)	30
8.2	Outsourcing	31
8.3	Cross-border System Support	31
 GLOSSARY AND ACRONYMS		 32
 ANNEXURE 1		 35
 ANNEXURE 2		 36
 ANNEXURE 3		 37
 ANNEXURE 4		 38

Chapter 1

1. Introduction

The banking industry has changed the way they provide services to their customers and process information in recent years. Information and Communication Technology (ICT) has brought about this momentous transformation. Security of Information for a financial institution has therefore gained much importance, and it is vital for us to ensure that the risks are properly identified and managed. Moreover, information and information technology systems are essential assets for the banks as well as for their customers and stakeholders. Information assets are critical to the services provided by the banks to their customers. Protection and maintenance of these assets are critical to the organizations' sustainability. Banks must take the responsibility of protecting the information from unauthorized access, modification, disclosure and destruction.

Bangladesh Bank has prepared a Guideline for ICT Security for banks & FIs to be used as a minimum requirement and as appropriate to the level of computerization of their operations.

1.1 Scope

This ICT Security Guideline is a systematic approach to policies required to be formulated for ensuring security of information and information systems.

This Guideline covers all information that are electronically generated, received, stored, printed, scanned, and typed. The provisions of this Guideline are applicable for:

- Scheduled banks & FIs for all of their Information Systems.
- All activities and operations required to ensure data security including facility design, physical security, network security, disaster recovery and business continuity planning, use of hardware and software, data disposal, and protection of copyrights and other intellectual property rights.

1.2 Objectives

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

- To establish a standard ICT Security Policy & ICT Security Management
- To help the banks and FIs for secured and stable setup of its ICT platform
- To establish a secured environment for the processing of data
- To identify information security risks and their management
- To communicate the responsibilities for the protection of information
- To prioritize information and information systems those need to be protected
- To aware and train the users associated with managing the ICT infrastructure
- To explain procedure for periodic review of the policy and security measures
- To ensure the best practices (industry standard) of the usage of ICT that is not limited to this guideline.

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

The locations for which the ICT Security Guideline is applicable i.e., the Head Office, Zonal Office, Branch and/or Booth/Unit of a bank or FI 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 and booths are connected through WAN with 24x7 hours attended operation.

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

Tier-3: Head Office, Zonal Office, Branch or booth having standalone computer(s).

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

Chapter 2

2. ICT Security Management

ICT Security Management must ensure that the ICT functions and operations are efficiently and effectively managed. They should be aware of the capabilities of ICT and be able to appreciate and recognize opportunities and risks of possible abuses. **They have to ensure maintenance of appropriate systems documentations, particularly for systems, which support financial reporting.** They have to participate in ICT security planning to ensure that resources are allocated consistent with business objectives. They have to ensure that sufficient and qualified technical staffs are employed so that continuance of the ICT operation area is unlikely to be seriously at risk all times.

ICT Security Management deals with ICT Security Policy Documentation, Internal Information System Audit, Training and Insurance. ICT security planner and/or steering committee shall be responsible for overall ICT security management.

2.1 ICT Security Policy

2.1.1 Every bank having Information systems must have an 'ICT Security Policy' which must be fully complied with this ICT Security Guideline and be approved by the board of the bank. For foreign banks, the documents must also be in conformity with their global policy documents.

This document provides the guideline for Information System and its secured usage for the banks. It establishes general requirements and responsibilities for protecting Information and Information System. The policy covers common technologies such as computers & peripherals, data and network, web system, and other specialized ICT resources. The bank's delivery of services depends on availability, reliability and integrity of its information technology system. Therefore, each bank must adopt appropriate methods to protect its information system. The senior management of the bank must express a commitment to ICT security by continuously increasing awareness and ensuring training of the bank's staff.

The policy will require regular update to cope with the evolving changes in the ICT environment both within the bank and overall industry.

2.1.2 For noncompliance issues, compliance plan shall be submitted to Bangladesh Bank for dispensation as per format given in **Annexure 1**.

2.2 Documentation

2.2.1 The following shall be documented:

- a) Organogram chart for ICT department/division (centralized/ decentralized)
- b) Branch organogram with the ICT support unit/section/personnel (Business/ICT)
- c) Job description (JD) for each individual within ICT department/ division
- d) A scheduled roster for personnel doing shifting duties
- e) Segregation of duties for IT tasks
- f) Fallback plans for various levels of system support personnel

2.3 Internal Information System Audit

2.3.1 Internal Information System Audit shall be carried out by Internal Audit or relevant Department (other than ICT Department).

2.3.2 Internal Audit Team should have sufficient ICT expertise/resources capable of conducting Information System Audit.

2.3.3 Internal Information System audit shall be done periodically at least once a year. The report must be preserved for Bangladesh Bank officials as and when required. An annual system audit plan shall be developed. Banks shall also ensure that audit issues are properly tracked and, in particular, completely recorded, adequately followed up and satisfactorily rectified.

2.3.4 The bank/branch shall take appropriate measures to address the recommendations made in the last Audit Report. This must be documented and kept along with the Audit Report mentioned in 2.3.3.

2.4 Training and Awareness

2.4.1 Bank shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the ICT security activities as relevant with their job function.

2.4.2 Bank shall also ensure the minimum level of Business Foundation Training for ICT personnel.

2.5 Insurance or Risk Coverage Fund

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

2.6 Problem Management

2.6.1 Bank shall establish a process to log the information system related problems and incidents.

2.6.2 Process shall have the workflow to assign the issue to a concerned person to get a quick, effective and orderly response.

2.6.3 Process shall be established to perform necessary corrective action within the time frame according to the problem's severity.

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

2.6.5 Process shall be established to review and monitor the incidents.

2.7 Risk Management

2.7.1 Effective risk management system shall be in place for any new processes and systems as well as a post-launch review.

2.7.2 The risk management function shall ensure awareness of, and compliance with, the ICT security control policies, and to provide support for investigation of any ICT related frauds and incidents.

2.7.3 The risk management process shall include:

- a) A description and assessment of the risk being considered and accepted for acknowledgement by the owner of the risk;
- b) Identification of mitigation controls;
- c) Formulation of a remedial plan to reduce the risk;
- d) Approval of the risk acknowledgement from the owner of the risk and senior management.

Chapter 3

3. ICT Operation Management

ICT Operation Management covers the dynamics of technology operation management including change management, asset management, operating procedures and request management. The objective is to achieve the highest levels of technology service quality by minimum operational risk.

3.1 Change Management

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

3.1.2 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**.

3.1.3 Audit logs of changes shall be maintained.

3.1.4 User Acceptance Test (UAT) for changes and upgrades in application shall be carried out before deployment. A sample form for UAT has been given in **Annexure 3**.

3.2 Asset Management

3.2.1 Assets shall be clearly identified and an inventory with significant details must be maintained.

3.2.2 All assets associated with the information facilities must be labeled with tag and name.

3.2.3 Asset inventory must be reviewed at least once a year.

3.2.4 All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or reissue.

3.2.5 Bank must comply with the terms of all software licenses and must not use any software that has not been legally purchased or otherwise legitimately obtained.

3.2.6 Software used in production environment must be subjected to a support agreement.

3.2.7 Software used in any computer must be approved by the authority. Use of unauthorized or pirated software must strictly be prohibited throughout the bank. Random checks shall be carried out to ensure compliance.

3.3 Operating Procedures

3.3.1 Operating procedures shall be documented, maintained and available for the users related to their job function.

3.3.2 Changes to operating procedures must be approved by management and documented.

3.3.2 Operating procedures shall cover the followings where appropriate:

- a) Documentation on handling of different processes;
- b) Documentation on scheduling processes, system start-up, close-down, restart and recovery (centralized/decentralized);
- c) Documentation on handling of exception conditions;
- d) Schedule system maintenance.

3.4 Request Management

3.4.1 To avail any service related to ICT, a formal request process must be established. A sample form has been provided in **Annexure-4**.

Chapter 4

4. Physical Security

Bank requires that sound business and management practices be implemented in the workplace to ensure that information and technology resources are properly protected. It is the responsibility of each department to protect technology resources from unauthorized access in terms of both physical hardware and data perspectives. In fact, the effective security measure for assets in the workplace is a responsibility held jointly by both management and employees.

Physical security involves providing environmental safeguards as well as controlling physical access to equipment and data. The following safeguard methods are believed to be practical, reasonable and reflective of sound business practices.

4.1 Physical Security for Tier-1

4.1.1 Data Center Access

- 4.1.1.1 Physical security shall be applied to the information processing area or Data Center.
- 4.1.1.2 Data Center must be a restricted area and unauthorized access shall be prohibited.
- 4.1.1.3 Entrance into the Data Center shall be restricted.
- 4.1.1.4 Access authorization procedures shall exist and be applied to all persons (e.g. employees and vendors). Unauthorized individuals and cleaning crews must be escorted during their stay in the Data Center.
- 4.1.1.5 Access authorization list shall be maintained and reviewed periodically for the authorized person to access the Data Center.
- 4.1.1.6 Access log with date, time and purpose shall be maintained for the vendors, service providers and visitors entered into the Data Center.
- 4.1.1.7 Security guard shall be available for 24 hours.
- 4.1.1.8 Emergency exit door shall be available.

4.1.2 Environmental Security

- 4.1.2.1 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.
- 4.1.2.2 Physical layout of Data Center including power supply and network connectivity shall be documented.
- 4.1.2.3 Development and test environment shall be separated from production.
- 4.1.2.4 Raised floor with removable blocks or channels alongside the wall shall be prepared to protect data and power cables from interception and any sort of damages.
- 4.1.2.5 Water detection devices shall be placed below the raised floor, if it is raised.
- 4.1.2.6 Any accessories not related/associated to Data Center shall not be allowed to store in the Data Center.
- 4.1.2.7 Closed Circuit Television (**CCTV**) camera shall be installed for monitoring.
- 4.1.2.8 The sign of "**No eating, drinking or smoking**" shall be in display.
- 4.1.2.9 Dedicated office vehicles for any of the emergencies shall always be available on site. Availing of public transport must be avoided while carrying critical equipments outside the bank's premises to avoid the risk of any causality.
- 4.1.2.10 Data Center shall have dedicated full-time supported telephone communication.
- 4.1.2.11 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 cope with any emergency situation.
- 4.1.2.12 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.

4.1.2.13 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.

4.1.2.14 The following environmental controls shall be installed:

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

The above shall be regularly tested and maintenance service contract shall be for 24x7 basis.

4.1.3 Fire Prevention

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

4.1.3.2 Fire suppression equipments shall be installed.

4.1.3.3 Automatic fire alarming system shall be installed and tested periodically.

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

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

4.1.3.6 Any flammable items shall not be kept in the Data Center.

4.2 Physical Security for Tier-2

4.2.1 Server Room Access

4.2.1.1 Server room must have a glass enclosure with lock and key with a responsible person of the Branch.

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

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

4.2.2 Environmental Security

4.2.2.1 Server must have password protected screen saver that shall be activated after a period as per bank's policy.

4.2.2.2 There shall be a provision to replace the server within shortest possible time in case of any disaster.

4.2.2.3 Server room shall be air-conditioned.

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

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

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

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

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

- 4.2.2.9 Proper earthing of electricity shall be ensured.
- 4.2.2.10 Address and telephone or mobile 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.

4.2.3 Fire Protection

- 4.2.3.1 Power supply must be switched off before leaving the server room.
- 4.2.3.2 Fire extinguisher shall be placed outdoor of the server room. This must be maintained and checked on an annual basis.

4.3 Physical Security for Tier-3

4.3.1 Computer Room Access

- 4.3.1.1 The PC running the branch banking software must be placed in a secured area and held by a responsible person in the Branch.
- 4.3.1.2 Access authorization list must be maintained and reviewed on a regular basis.

4.3.2 Environmental Security

- 4.3.2.1 PC must have password-protected screensaver which shall be activated after a period as per bank's policy.

4.3.3 Fire Protection

- 4.3.3.1 Preventive measures shall be taken to protect computer room from short circuits.
- 4.3.3.2 Power and other connecting cables for PCs must be kept secured from physical damage.
- 4.3.3.3 Power supply of the PC shall be switched off before leaving the branch.

4.3.3.4 Fire extinguishers with expiry date shall be placed beside the power distribution board. This must be maintained and checked on an annual basis.

4.3.3.5 Proper earthing of electricity shall be ensured.

4.4 Physical Security for Desktop and Laptop Computers

4.4.1 Desktop computer shall be connected to UPS to prevent damage of data and hardware.

4.4.2 Before leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature.

4.4.3 Password protected screen saver shall be used to protect desktop and laptop from unauthorized access.

4.4.4 Laptop computers that store confidential or sensitive information must have encryption technology.

4.4.5 Desktop and laptop computers and monitors shall be turned off at the end of each workday.

4.4.6 Laptop computers, computer media and any other forms of removable storage (e.g. diskettes, CD ROMs, zip disks, PDAs, flash drives) shall be stored in a secured location or locked cabinet when not in use.

4.4.7 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.

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

4.4.9 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).

4.4.10 Any kind of viruses shall be reported immediately.

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

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

- 4.4.13 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.
- 4.4.14 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.)
- 4.4.15 All computers shall be placed above the floor level and away from windows.

Chapter 5

5. Information Security Standard

The objective of this chapter is to specify Information Security Policies and Standards to be adopted by all scheduled banks in Bangladesh using Information and Communication Technology for service delivery and data processing. This chapter covers the basic and general information security controls applicable to all functional groups of a business to ensure that information assets are protected against risk.

5.1 Access Control for Information Systems

5.1.1 User ID Maintenance

- 5.1.1.1 Each user must have a unique User ID and a valid password.
- 5.1.1.2 User ID shall be locked up after 3 unsuccessful login attempts.
- 5.1.1.3 User ID and password shall not be same.
- 5.1.1.4 User ID Maintenance form with access privileges shall be duly approved by the appropriate authority.
- 5.1.1.5 Access privileges shall be changed/ locked within 24 hours or as per bank's policy when users' status changed or user left the bank.

5.1.2 Password Control

- 5.1.2.1 The password definition parameters ensure that minimum password length is specified according to the Bank's ICT Security Policy (at least 6 characters, combination of uppercase, lowercase, numbers & may include special characters).
- 5.1.2.2 Administrative password of Operating System, Database and Banking Application shall be kept in sealed envelope and kept in a safe custody (centralized/decentralized).
- 5.1.2.3 The maximum validity period of password shall not be beyond the number of days permitted in the Bank's ICT Security Policy (within 30 to 90 days cycle).

- 5.1.2.4 The parameters to control the maximum number of invalid logon attempts shall be specified properly in the system according to the ICT Security Policy of the Bank (maximum 3 consecutive times).
- 5.1.2.5 Password history maintenance shall be enabled in the system to allow same passwords to be used again after at least 4 times.
- 5.1.2.6 Session time-out period for users shall be set in accordance with the bank's Policy.
- 5.1.2.7 Operating time schedule for the users shall be defined where necessary.
- 5.1.2.8 Audit trail shall be available to review the user profile in the application.

5.1.3 Input Control

- 5.1.3.1 Software shall not allow the same user to be both maker and checker of the same transaction. Management approval must be in place for delegation of authority.
- 5.1.3.2 Audit trail must be clearly marked with User Id and date-time stamp.
- 5.1.3.3 The system shall be restricted from being accessed especially in sensitive data/fields.

5.2 Network Security

- 5.2.1 The Network Design and its security shall be implemented under a documented plan.
- 5.2.2 Physical security for the network equipments shall be ensured. Specifically:
 - a) Access shall be restricted and controlled.
 - b) Network equipments shall be housed in a secure environment.
- 5.2.3 Groups of information services, users, and information systems shall be segregated in networks, e.g. VLAN.

- 5.2.4 Unauthorized access and electronic tampering shall be controlled strictly.
- 5.2.5 Firewall shall be in place on the network for any external connectivity.
- 5.2.6 Redundant communication links shall be used for WAN.
- 5.2.7 There shall be a system to detect unauthorized intruder in the network.
- 5.2.8 Connection of personal laptop to office LAN or any personal wireless modem with the office laptop/desktop must be secured.

5.3 Data Encryption

- 5.3.1 Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.

5.4 Virus Protection

- 5.4.1 Anti-virus software shall be installed in each server and computer whether it is connected to network or not.
- 5.4.2 Virus auto protection mode shall be enabled.
- 5.4.3 Anti-virus software shall always be updated with the latest virus definition file.
- 5.4.4 All computers in the network shall get updated signature of anti-virus software automatically from the server.
- 5.4.5 Bank may arrange awareness program for the users about computer viruses and their prevention mechanism.

5.5 Internet and e-mail

- 5.5.1 All Internet connections shall be routed through a firewall for computers connected to network and Anti-Virus Gateway like Web-Shield, Trend Micro etc. to get protection from spam, worm, Trojan etc. that is accessing in bank's network while browsing, downloading, or an attachment of any incoming mail to the PCs connected to bank's network.

- 5.5.2 Access to e-mail system and internet shall only be obtained through official request.
- 5.5.3 E-mail system and internet shall be used according to the bank's policy.
- 5.5.4 Concerned department shall perform regular review and monitoring of e-mail service.
- 5.5.5 Users shall not use profanities, obscenities, or derogatory remarks in e-mail messages regarding employees, customers, competitors, or others.
- 5.5.6 All attachments with the incoming e-mail messages shall be monitored especially for viruses.
- 5.5.7 Mail server must have latest anti-virus signature.

5.6 Transactions through Alternative Channels

5.6.1 Services through Mobile

Controls over mobile transaction are required to manage the risks of working in an unprotected environment. Therefore, banks shall establish following control procedures to ensure confidentiality, integrity, authenticity and non-repudiability:

- 5.6.1.1 Security standards shall be followed appropriate to the complexity of services offered.
- 5.6.1.2 Appropriate risk mitigation measures shall be implemented like transaction limit, transaction frequency limit, fraud checks, AML checks etc. depending on the risk perception, unless otherwise mandated by the regulatory body.
- 5.6.1.3 Services provided by banks through mobile shall comply with security principles and practices for the authentication of transactions mandated by the regulatory body.
- 5.6.1.4 Proper level of encryption and security shall be implemented at all stages of the transaction processing. The following measures with respect to network and system security shall be adhered to:
 - a) Implement application level encryption over network and transport layer encryption wherever possible.

- b) Establish proper firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), data file and system integrity checking, surveillance and incident response procedures.
- c) Conduct periodic risk management analysis, security vulnerability assessment of the application and network at least once a year.

5.6.1.5 Bank shall comply with '*Regulatory Compliance*' requirements of the country.

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

5.6.2 Internet Banking

Information involved in internet banking passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification. Therefore, bank shall establish following control procedures:

5.6.2.1 I-banking standards shall be included in the Bank's ICT Security Policy.

5.6.2.2 Network and Database administrator shall ensure the security issues of I-banking.

5.6.2.3 Bank shall introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards, biometric technologies or other industry standards.

5.6.2.4 Bank shall ensure real time security log for unauthorized access.

5.6.2.5 Bank shall define technology security protocols for I-banking solutions like PKI (Public Key Infrastructure), SSL (Secured Socket Layer), 2-FA (Two Factor Authentication), RSA, VASCO etc.

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

5.6.2.7 The information security officer, system auditor or any other concerned 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) & DoS (Denial of Service) attacks.
- d) Checking of commonly known holes in the software, especially the browser and the e-mail software exist.
- e) Checking the weaknesses of the infrastructure.
- f) Taking control of ports.
- g) Cause application crash.
- h) Injecting malicious codes to application and database servers.

5.6.2.8 All applications of bank shall have proper record keeping facilities for legal purposes. Bank may keep all received and sent messages in restricted form.

5.6.2.9 Security infrastructure shall properly be tested before using the systems and applications for normal operations. Banks might upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

5.6.3 Payment Cards

Bank providing the payment card services must comply with the industry security standards, e.g.- Payment Card Industry Data Security Standard (PCI DSS) to ensure the security of cardholder's data. The PCI DSS includes following requirements for security management, policies, procedures, network architecture, software design and other protective measures:

5.6.3.1 PINs used in transactions shall be processed using equipment and methodologies to ensure that they are kept secured.

- 5.6.3.2 Cryptographic keys used for PIN encryption/decryption and related key management shall be created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.
- 5.6.3.3 Secret or private Keys shall be conveyed or transmitted in a secured manner.
- 5.6.3.4 Unencrypted Key loading to hosts and PIN entry devices shall be handled in a secured manner.
- 5.6.3.5 Randomized Keys shall be used in a manner that prevents or detects their unauthorized usage.
- 5.6.3.6 Keys shall be administered in a secured manner.
- 5.6.3.7 Equipment used to process PINs and keys shall be managed in a secured manner.

Chapter 6

6. Software Development and Acquisition

For any new application or function for the bank requires analysis before acquisition or creation 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'.

6.1 In-house Software

- 6.1.1 Detailed design and technical application requirements shall be prepared.
- 6.1.2 Criteria for acceptance of the requirement shall be defined and approved by the concerned business unit.
- 6.1.3 Application security and availability requirements shall be addressed.
- 6.1.4 Developed functionality in the application shall be in accordance with design specification and documentation.
- 6.1.5 Source code must be available with the concerned department and kept secured.
- 6.1.6 Source code shall contain title area, the author, date of creation, last date of modification and other relevant information.
- 6.1.7 Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall be followed and conducted in the development and implementation stage.
- 6.1.8 System documentation and User Manual shall be prepared and handed over to the concerned department.
- 6.1.9 Necessary '*Regulatory Compliance*' requirements must be taken into account by the Bank.

6.2 Outsourced Software

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

6.2.1 Vendor Selection

6.2.1.1 There must be a core team comprising of personnel from Functional Departments, IT Department and Internal Audit Department for vendor selection.

6.2.1.2 Vendor selection criteria for application must address the following:

- a) Market presence
- b) Years in operation
- c) Technology alliances
- d) Extent of customization and work around solutions
- e) Performance & Scalability
- f) Number of installations
- g) Existing customer reference
- h) Support arrangement

6.2.2 Software Documentation

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

6.2.2.2 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

6.2.3 Other Requirements

- 6.2.3.1 There shall have a test environment to ensure the software functionalities before implementation.
- 6.2.3.2 User Acceptance Test shall be carried out and signed-off before going live.
- 6.2.3.3 Necessary 'Regulatory Compliance' requirements for banking procedures and practices in the application must be taken into account by the Bank.
- 6.2.3.4 Any bugs and/or errors found due to design flaws, must be escalated to higher levels in Software Vendors' organization and bank, and must be addressed in time.
- 6.2.3.5 Support agreement must be maintained with the provider for the software used in production with the confidentiality agreement.

Chapter 7

7. Business Continuity and Disaster Recovery Plan

Business Continuity Plan (BCP) is required to cover operational risks and takes into account the potential for wide area disasters, Data Center disasters and the recovery plan. The primary objective of BCP is to enable a bank to survive a disaster and to re-establish normal business operations. In order to survive, bank shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the business resumption planning and disaster recovery planning.

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

7.1 Business Continuity Plan (BCP)

7.1.1 Bank must have a Business Continuity Plan addressing the recovery of disaster to continue its operation.

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

7.1.3 BCP shall address the followings:

- a) Action plan to restore business operations within the required time frame: i) during office hour's disaster, ii) outside office hour's disaster, and iii) immediate and long term plan.
- b) Emergency contacts, addresses and phone numbers including vendors
- c) Grab list of items such as backup tapes, laptops, flash drives etc.
- d) Disaster recovery site map

7.1.4 BCP must be tested and reviewed regularly to ensure the effectiveness.

7.2 Disaster Recovery Plan (DRP)

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

7.3 Backup and Restore Plan (BRP)

- 7.3.1 There shall be a documented backup procedure.
- 7.3.2 Bank shall ensure the safety and security of the backup copies of information from not being damaged by natural calamities and theft (if possible to be sent at off-site location).
- 7.3.3 At least one copy of backup shall be kept on-site for the time critical delivery.
- 7.3.4 The backup shall be done periodically considering the cycle of:
 - a) Weekly, b) Monthly, c) Yearly or as required by regulatory authority.

- 7.3.5 The backup log sheet shall be maintained, checked & signed by supervisor.
- 7.3.6 The backup inventory shall be maintained, checked & signed by supervisor.
- 7.3.7 The ability to restore from backup media shall be tested at least quarterly.
- 7.3.8 Backup media must be labeled (soft/hard format) properly indicating contents, date etc.

Chapter 8

8. Service Provider Management

8.1 Service Level Agreement (SLA)

8.1.1 There shall be Service Level Agreement between the vendor and bank.

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

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

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

- a) Pricing
- b) Measurable service/deliverables
- c) Timing/schedules
- d) Confidentiality clause
- e) Contact person 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) Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies
- l) Geographical locations covered

- m) Ownership of hardware and software
- n) Documentation (e.g. logs of changes, records of reviewing event logs)
- o) Right to have information system audit conducted (internal or external).

8.2 Outsourcing

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

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

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

8.3 Cross-border System Support

8.3.1 The bank shall provide official authorization/assurance from the group ensuring the data availability and continuation of services for any circumstances e.g. diplomacy changes, natural disaster, relationship breakdown, discontinuity of services, or others.

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

Glossary and Acronyms

2-FA	- Two Factor Authentication
AMC	- Annual Maintenance Contract
AML	- Anti-Money Laundering
BCP	- Business Continuity Plan
BRP	- Backup and Restore Plan
CCTV	- Close Circuit Television
CD ROM	- Compact Disk Read Only Memory
DC	- Data Center
DDoS	- Distributed Denial of Service
DoS	- Denial of Service
DR	- Disaster Recovery
DRP	- Disaster Recovery Plan
DRS	- Disaster Recovery Site
E-mail	- Electronic Mail
FIs	- Financial Institutions
I-banking	- Internet Banking
ICT	- Information and Communication Technology
IDS	- Intrusion Detection System
IPS	- Intrusion Prevention System
IT	- Information Technology
JD	- Job Description

LAN	- Local Area Network
PCI DSS	- Payment Card Industry Data Security Standard
PCs	- Personal Computers
PDA	- Personal Digital Assistant
PIN	- Personal Identification Number
PKI	- Public Key Infrastructure
SDLC	- Software Development Life Cycle
SLA	- Service Level Agreement
SSL	- Secured Socket Layer
UAT	- User Acceptance Test
UPS	- Uninterrupted Power Supply
User ID	- User Identification
VLAN	- Virtual Local Area Network
WAN	- Wide Area Network

Annexure

(Sample)

Annexure 1 Dispensation Form

Reference:

Date:

Section I : Requester Information

Bank Name :
Branch/Division Name :
Requested by :
Requestor's Designation :
Requestor's Telephone :
Request Date :

Section II : Risk Overview

Guideline reference (Clause) and description :

.....
.....

Risk Details (Process/Application/System/Product) :

.....
.....

Justification :

Plan of mitigation :

.....
.....

Mitigation Date :

Section III : Approvals

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

Name :
Designation :
Comments :
Date :

Signature & Seal :

Annexure 2 Change Request Form

Reference:

Date:

Section I : Requester Information

Branch/Division Name :
Submitted by :
Change Description :
Change Purpose :
Request Date :

Signature & Seal
(Requester)

Signature & Seal
(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 Request Form

Reference:

Date:

Section I : Requester Information

Branch/Division Name :
Submitted by :
Contact No. :
Request Details :
Justification :
Request Date :

Signature & Seal
(Requester)

Signature & Seal
(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.

Request Reference No. :
Date of Request Implementation :
Request Implementation Details:

Was Request done successfully? Yes No

Name :
Designation :
Signature & Seal :