Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions

October, 2005

Bangladesh Bank

Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions

The Banking and Financial Industry has undergone varying degrees of transformation by moving their operating systems to Information Technology platforms. Notwithstanding the level of computerization the security requirement of these systems are universal and are critical to the sustainability of the platforms.

To address this requirement Bangladesh Bank has taken the initiative to provide the industry with a guideline of ‘minimum’ security standards.

This Guideline has been prepared by a Focus Group drawn from the industry and Bangladesh Bank.

I would like to thank all the members of the Focus Group for their contribution and in particular the Governor for his valuable guidance.

Muhammad A. (Rumee) Ali
Deputy Governor

Focus Group

Coordinator

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

Members

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

Abu Farah Md. Naser
Joint Director
Department of Banking Inspection-1
Bangladesh Bank

Moinuddin Ahmed
Deputy General Manager
Information Technology Division
Agrani Bank.

M Abul Kalam Azad
Head of Information Technology
Standard Chartered Bank

Khawja Muhammad Masum Billah
Vice President & Senior Country Operation Officer
Citibank, N.A.

Jamshed Atique
Manager
Information Technology
HSBC

Abul Kashem Md. Shirin
Executive Vice President and Head of IT
Dutch-Bangla Bank Limited

Muhammed Anwarul Islam
First Assistant Vice President & Manager Branch Support
Eastern Bank Limited

Contents

Chapter 1

1. Introduction

The banking industry has changed in the way they provide service to their customers and process information in recent years. Information Technology has brought about this momentous transformation. Security of IT systems for a financial institution has therefore gained much greater in importance, and it is vital that we ensure that such risks are properly identified and managed. Moreover Information and information technology systems are essential assets of the banks and as well as for their customers and stake-holders. 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 to protect customers' interest.

Bangladesh Bank has prepared a Guideline for Information & Communication Technology (ICT) for banks to be used as a minimum requirement and as appropriate to the level of computerization of their operations.

1.1 Scope

This IT Guideline is a systematic approach to policies required to be formulated for IT and also to ensure security of information and information systems.

This Guideline covers all information that is electronically generated, received, stored, printed, scanned, and typed. The provisions of this Guideline apply to:

• Scheduled banks for all of their IT 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 IT Policy & IT Management
- To help the bank for secure and stable setup of its IT platform
- To establish a secure environment for the processing of data
- To identify information security risks and their management
- To communicate the responsibilities for the protection of information
- Prioritize information and information systems that are to be protected
- User awareness and training regarding information security
- Procedure for periodic review of the policy and security measures

1.3 Categorization of banks depending on ICT operation

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

Tier-1: Centralized IT Operation of Data Center including Disaster Recovery Site (DRS) to which all other offices, branches and booths are connected through WAN. 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 stand alone computer(s) or ATM(s).

The proposed IT Guideline will be applicable for all the three tiers if not mentioned specifically.

Chapter 2

2 IT Management

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

IT Management deals with IT policy Documentation, Internal IT Audit, Training and Insurance.

2.1 ICT Policy

2.1.1 Every bank having IT systems must have an 'IT POLICY' which must fully comply with this IT Guideline and be approved by the Board of the bank. For foreign banks the document must also be in conformity with their global policy document.

This document will provide the policy for Information & Communication Technology and ensures its secured use for the banks. It establishes general requirements and responsibilities for protecting ICT systems. The policy covers such common technologies such as computers & peripherals, data and network, web system, and other specialized IT 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 technology system. The policy will require regular updates to cope with the evolving changes in the IT environment both within the bank and overall industry. The senior management of the bank must express a commitment to IT security by continuously upgrading awareness and ensuring training of the banks staff.

2.1.2 Compliance Plan in case of noncompliance issues.

2.1.3 For any dispensation bank must apply to Bangladesh Bank as per format given in **Annexure 1.**

2.2 Documentation

The following will be documented properly:

a) Organogram chart for IT department
b) Job description (JD) for each individual within IT department
c) A scheduled roster for IT operation
d) Segregation of duties for IT tasks
e) Fallback plans for various levels of system support personnel

2.3 Internal IT Audit

2.3.1 Internal Audit should have sufficient IT expertise / resources capable of conducting IT Audit.

2.3.2 Internal IT audit should be done periodically at least once a year. The report must be preserved for inspection of Bangladesh Bank officials as and when required.

2.3.3 The bank/branch should 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 2.3.2.

2.4 Training

2.4.1 Related employees should be given adequate training on sensitive IT Tasks.

2.4.2 The employees should be trained on aspects of importance and awareness of IT.

2.4.3 IT personnel should be trained on the necessary steps to be taken in case of any contingency/ health security in the IT area.

2.4.4 All the network users are trained about its operating and security procedures.

2.5 Insurance

2.5.1 Adequate insurance coverage should be provided under the bank's insurance policies (unless otherwise covered by the Group HQs in case of foreign banks) so that costs of loss and/or damage the hardware assets related to IT are minimized.

2.6 Problem Management

2.6.1 Log problem in daily/weekly basis.

2.6.2 Accept responsibility for problem resolution, and assign the problem internally to a team member for action.

2.6.3 Investigate the problem report.

2.6.4 Perform the necessary corrective action within the time frame bounded by the problem’s severity.

2.6.5 Document findings and action steps taken during the problem resolution process.

2.6.6 Provide remote systems problems information to specific support units and Regional Help Desk & Support Teams.

2.6.7 Provide time-to-time communication support to remote support units and getting solution.

Chapter 3

3. IT Operation Management

IT Operation Management covers the dynamics of technology operation management including change management, asset management, operating environment 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 All change implemented in the production environment must be governed by a formal documented process including forms with necessary change details. A sample form has been provided in **Annexure 2.**

3.1.2 Audit Logs of changes should be maintained available for ready references.

3.1.3 Signed off from the vendor should be obtained before implementation of changes in production.

3.1.4 User Acceptance Test (UAT) should be completed before change (Application related) implementation. A sample form for UAT has been given in **Annexure 3.** This document should be preserved for ready reference.

3.2 Asset Management

3.2.1 An inventory must be kept with all significant details for hardware and software and reviewed at least once a year. A record of this review must be maintained.

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

3.2.3 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.

3.2.4 Software used in production environments must be subject to a support agreement.

3.2.5 Software used in any computer must be approved by the authority. Use of unauthorized or pirated software must be strictly prohibited throughout the bank, particularly in networked PCs. Random checks should be carried out to ensure compliance.

3.3 Operating Procedures

3.3.1 Operating procedures must exist for all ICT functions.

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

3.3.3 Operating procedures cover the following where appropriate:

a. Documentation on handling of different process
b. Scheduling processes (including target start and finish times)
c. Documentation on handling of error and exception conditions
d. Documentation for secure disposal of output from failed processing runs
f. Documentation on system start-up, close-down, restart and recovery
g. Schedule system maintenance

3.4 Request Management

3.4.1 Before any IT service 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 of 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 list of safeguards methods where believed to be practical, reasonable and reflective of sound business practices.

4.1 Physical Security Guideline for Tier-1

4.1.1 Data Centre Access

4.1.1.1 Data Centre must be restricted area and unauthorized access is prohibited.

4.1.1.2 Number of entrance into the Data Centre should be limited, locked and secured.

4.1.1.3 Access Authorization procedures should exist and apply to all persons (e.g employees and vendors). Unauthorized individuals and cleaning crews must be escorted during their stay in the Data Centre.

4.1.1.4 Bank should maintain Access Authorization list, documenting individuals who are authorized to access the data centre, reviewed and updated periodically.

4.1.1.5 Access log with date and time, should be maintained documenting individuals who have accessed the data centre.

4.1.1.6 Visitor Log should exist and need to be maintained.

4.1.1.7 Security guard should be available for 24 hours.

4.1.1.8 There should be Emergency exit door available.

4.1.2 Environmental

4.1.2.1 Sufficient documentation is required regarding the physical layout of the data centre.

4.1.2.2 Documentation regarding the layout of power supplies of the data centers and network connectivity to be prepared.

4.1.2.3 Floors to be raised with removable square blocks or channel alongside the wall to be prepared, which allow all the data and power cabling to be in neat and safe position.

4.1.2.4 Water detection devices should be below the raised floor, if it is raised.

4.1.2.5 Any accessories, not related to data center should not be allowed to be stored in the Data Centre.

4.1.2.6 Existence of Closed Circuit Television **(CCTVs)** camera is required and to be monitored.

4.1.2.7 Data Centre must show the **sign of "No eating, drinking or smoking."**

4.1.2.8 Vehicles for any emergency purpose should always be available on site.

4.1.2.9 Address and telephone or mobile numbers of all contact persons (e.g. Fire service, police station, service providers, vendor and all IT personal) should be available to cope with any emergency situation.

4.1.2.10 Proper attention must be given with regard to overloading of electrical outlets with too many devices. Proper and practical usage of extension cords should be reviewed annually in the office environment.

4.1.2.11 The following computer environmental controls to be installed:

a) Uninterruptible power supply (UPS) with backup units
b) Backup Power Supply
c) Temperature and humidity measuring devices
d) Air conditioners with backup units
e) Water leakage precautions and water drainage system from Air conditioner
f) Emergency power cut-off switches
g) Emergency lighting arrangement
h) Dehumidifier to be installed

Determine if the above are regularly tested and that maintenance of service contracts exists on 24x7x365 basis.

4.1.3 Fire Prevention

4.1.3.1 The Data Centre wall/ceiling/door should be fire resistant.

4.1.3.2 Fire suppression equipment should be installed.

4.1.3.3 Procedures must exist for giving the immediate alarm of a fire, and reporting the fire services and to be periodically tested.

4.1.3.4 There should be Fire detector below the raised floor, if it is raised.

4.1.3.5 Electric cables in the Data Centre must maintain a quality and concealed.

4.1.3.6 Any flammable items should not be kept in the Data Centre.

4.2 Physical Security Guideline 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 should 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

4.2.2.1 Desktop screen must be locked and Server must have password protected screen saver that should activate after 10 seconds.

4.2.2.2 Administrative password of **Operating System** and **Database** should be written in sealed envelop and kept in vault.

4.2.2.3 User creation request form should be maintained.

4.2.2.4 Provision to replace the server within quickest possible time in case of any disaster.

4.2.2.5 Server room should be air-conditioned.

4.2.2.6 Power Generator should be in place to continue banking operations in case of power failure.

4.2.2.7 UPS should be in place to provide uninterrupted power supply to the server during power failure.

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

4.2.3 Fire Protection

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

4.2.3.2 Power supply must be switched off before leaving the Server room.

4.2.3.3 Fire extinguisher needs to be placed outdoor of the server room. This must be maintained and reviewed on an annual basis.

4.2.3.4 Proper earthing of electricity to be ensured.

4.3 Physical Security Guideline 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 glass enclosure with lock and key and **held by a responsible person in the Branch.**

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

4.3.2 Environmental

4.3.2.1 Operator must have the desktop password only known to him and kept written in sealed envelop in the vault.

4.3.2.2 PC must have password-protected screensaver which should activate after 1 minute of inactivity.

4.3.3 Fire Protection

4.3.3.1 Power distribution board for the PC with a **circuit breaker** should be placed outside the enclosure and covered with a box under lock and key **held by the Operator.**

4.3.3.2 Power and other connecting cables for PCs must be kept secured from physical damage.

4.3.3.3 UPS for backup power supply to be placed in the enclosure.

4.3.3.4 Power supply of the PC should be switched off before leaving the branch.

4.3.3.5 Fire extinguishers with expiry date mentioned, to be placed beside the Power distribution board. This must be maintained and reviewed on an annual basis.

4.3.3.6 Proper earthing of electricity to be ensured.

4.4 Physical Security for Desktop and Laptop computers

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

4.4.2 When leaving a desktop or laptop computer unattended, users shall apply the "*Lock Workstation*" feature (ctrl/alt/delete, enter) where systems allow.

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

4.4.4 Automatic screensaver should be activated after a period of inactivity. This period should not be more than five (5) minutes.

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

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

4.4.7 Laptop computers actively connected to the network or information systems must not be left unattended.

4.4.8 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 secure location or locked cabinet when not in use.

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

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

4.4.11 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).

4.4.12 Any kind of viruses should be reported immediately.

4.4.13 Viruses shall not be deleted without expert assistance unless instructed by the IT.

4.4.14 User identification (name) and authentication (password) shall be required to access all desktop and laptop whenever turned on or restarted.

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

4.4.16 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.)

4.4.17 On holiday occassions computers should be removed from floors and away from windows.

Chapter 5

5. Information Security Standard

The objective of this chapter is to specify Information Security Policies and Standard to be adopted by all scheduled banks in Bangladesh using Information Technology (IT) 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 Password Control

5.1.1.1 The password definition parameters ensure that minimum password length is specified according to the Bank's IT security policy of the bank (at least 6 characters, combination of uppercase, lowercase, numbers & special characters).

5.1.1.2 The maximum validity period of password is not beyond the number of days permitted in the Bank's IT Security policy (maximum 30 days cycle).

5.1.1.3 The parameters to control the maximum number of invalid logon attempts is specified properly in the system according to the IT security policy (maximum 3 consecutive times).

5.1.1.4 Password history maintenance is enabled in the system to allow same passwords can be used again after at least 4 times.

5.1.1.5 Password entries must be masked.

5.1.1.6 The terminal inactive time allowable for users should be set in accordance with the Bank's policy.

5.1.1.7 Operating time schedule for the users is to be defined where necessary.

5.1.1.8 Sensitive passwords have to be preserved in a sealed envelope with movement records for usage in case of emergency.

5.1.1.9 Audit trail should be available to review the user profile for maintenance purpose.

5.1.2 User ID Maintenance

5.1.2.1 Each user must have a unique UserID and a valid password.

5.1.2.2 The UserID will be locked up after 3 unsuccessful log in attempts.

5.1.2.3 There need to have a control to ensure that user ID and password are not same.

5.1.2.4 The UserID Maintenance Form with access privileges is duly approved by the appropriate authority.

5.1.2.5 Access privileges are changed/locked within 24 hours when users' status changed or left the bank.

5.1.3 Input Control

5.1.3.1 The software should not allow the same person to be both the maker and checker of the same transaction.

5.1.3.2 Audit trail must be clearly marked with userID and date-time stamp.

5.1.3.3 The system is restricted from being accessed specially sensitive data/fields.

5.2 Network Security

5.2.1 The Network Design and its security are implemented under a documented plan.

5.2.2 Physical security for the network equipment should be ensured.
Specifically: a. Access should be restricted and controlled. b. These should be housed in a secure environment.

5.2.3 The sensitive information should be kept in restricted area in the networking environment.

5.2.4 Unauthorized access and Electronic tampering is to be controlled strictly.

5.2.5 Security of the network should be under dual administrative control.

5.2.6 Firewalls are in place on the network for any external connectivity.

5.2.7 Redundant communication links are used for WAN.

5.2.8 There should be a system to detect the unauthorized intruder for network.

5.3 Data Encryption

5.3.1 There is mechanism in place to encrypt and decrypt the highly sensitive data traveling through WAN or public network.

5.4 Virus Protection

5.4.1 There should be Anti-Virus installed in each server and computer whether it is connected to LAN or not.

5.4.2 Virus auto protection mode is enabled.

5.4.3 The anti virus software is always updated with the latest virus definition file.

5.4.4 All users are well-trained and informed about computer viruses and their prevention mechanism.

5.4.5 There are procedures in place, which require that all the incoming e-mail messages are scanned for viruses to prevent virus infection to the bank’s network.

5.5 Internet and e-mail

5.5.1 All Internet connections should be routed through a Firewall for PCs connected to network.

Chapter 6

6. Business Continuity and Disaster Recovery Plan

The Business Continuity Plan (BCP) is required to cover operational risks and should take into account the potential for wide area disasters, data centre disasters and the recovery plan. The BCP should take into account the backup and recovery process. Keeping this into consideration this chapter covers BCP, Disaster Recovery Plan and Backup / Restore plan.

6.1 Business Continuity Plan (BCP)

6.1.1 There must be a Business Continuity Plan (in line with business) for IT in place.

6.1.2 All the documents related to business continuity and disaster recovery plan must be kept in a safe/secured off site location. One copy can be stored in the office for ready reference.

6.1.3 BCP must contains the followings:

a) Action plan for i) during office hours disaster, ii) outside office hours disaster, and iii) immediate and long term action plan in the line with business
b) Emergency contacts, address and phone numbers including venders
c) Grab list of items such as backup tapes, laptops etc.
d) Disaster recovery site map

6.1.4 Review of BCP must be done at least once a year/

6.2 Disaster Recovery Plan (DRP)

6.2.1 A Disaster Recovery Site (DRS) must be in place replicating the Data Center (Production Site).

6.2.2 DR site must be at a minimum of 10 kilometers (radius) of distance from the ‘production’ site.

6.2.3 DR site is equipped with compatible hardware and telecommunications equipment to support the live systems in the event of a disaster.

6.2.4 Physical and environmental security at the DR site is appropriate.

6.2.5 Information security is properly maintained throughout the fallback and DR recovery process.

6.2.6 An up-to-date and tested copy of the DR plan is securely held off-site. DR plans exists for all the critical services where DR requirement is agreed with the business.

6.2.7 DR test is successfully carried out at least once a year.

6.2.8 DR Test documentation should include at a minimum:

a) Scope - defines scope of planned tests - expected success criteria
b) Plan - detailed actions with timetable
c) Test Results

6.3 Backup / Restore

6.3.1 There is a documented back up procedure.

6.3.2 Backup copies of information is stored off-site at a geographically separate and safe environment.

6.3.3 There is at least one backup copy kept on-site for time critical delivery.

6.3.4 The backup cycle is based on the following:

a) At least 6-days (week) daily cycle
b) At least 6-month monthly cycle
c) Yearly cycle as required by regulatory authority

6.3.5 The back up media is sent off-site immediately after the back up have been taken.

6.3.6 The back up log sheet is maintained, checked & signed by supervisor

6.3.7 The back up inventory is maintained, checked & signed by supervisor.

6.3.8 The ability to restore from backup media is tested at least quarterly.

6.3.9 Backup Media must be labeled properly indicating contents, date etc.

Chapter 7

7. Service Provider Management

7.1 Service Level Agreement (SLA)

7.1.1 There should be Service Level Agreement between the vendor and bank.

7.1.2 The Annual Maintenance Contact (AMC) with the vendor should be active and currently in force.

7.1.3 The user site should ensure that the equipment does not contain sensitive live data when hardware are taken by the vendors for servicing / repair.

7.1.4 Service Contracts with all service providers including third-party vendors should include:

a) Pricing.
b) Measurable service/deliverables
c) Timing/schedules, i.e. service levels
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 to be maintained (e.g. logs of changes, records of reviewing event logs)
o) Audit rights of access (internal audit, external audit, other audit as may be appropriate).

7.2 Out Sourcing

Outsourcing activities to be evaluated based on the following practices:

a) The objective behind Outsourcing
b) The economic viability
c) The risks and security concerns
d) Arrangements for obtaining the source code for the software

Annexure

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 :