Internal Control & Compliance Division, Head Office, Dhaka

IT Audit Guidelines

For Internal Use Only

December 2017

IT Audit Guidelines

Table of Contents

Chapter No.	Chapter Name	Chapter Issued	Page Revised
1	**Introduction**	December 2016	-

Chapter: 1
Introduction

1.1 Introduction

The banking industry has changed in recent years; providing services to their customers by means of Information Technology and processing enhanced Management Information System (MIS). This technological development has brought momentous transformation in the banking arena. Security of IT systems for a financial institution has gained much greater importance and it is vital to ensure that risks are properly identified and managed. Adequate MIS and Information Technology systems are essential assets of the bank as well as for the customers and stakeholders.

Bank should take the necessary measures to protect the information from unauthorized access, modification, disclosure and destruction to protect customers' interest. To address the requirement of Bangladesh Bank in the field of IT Audit; Internal Control & Compliance Division has taken an initiative to provide the bank with the guidelines of adequate security standards and controls.

1.2 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:

- The United Commercial Bank Limited 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.

1.3 Objective

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;
- To formulate security requirements and objectives;
- To ensure compliance with laws and regulations;
- Definition of new information security management processes;
- Identification and clarification of existing information security management processes;
- To determine the status of information security management activities;
- To determine the degree of compliance with the policies, directives and standards adopted by the bank;

Chapter No.	Chapter Name	Chapter Issued	Page Revised
1	**Introduction**	**December 2016**	-

1.4 Categorization of banks depending on IT operation

The locations for which the IT Audit Guideline is applicable i.e., Head Office Divisions, Branches, Agent Banking Centers 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, Sales & Service Centers and booths are connected through WAN. 24x7 hours attended operation.

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

Tier-3:
Head Office, Regional Office, Sales & Service Centers or booth having stand alone computer(s) or ATMS (s).

The proposed IT Audit Guidelines will be applicable for the tier-1 if not mentioned specifically.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
2	**IT Auditing Procedures**	December 2016	-

Chapter: 2
IT Auditing Procedure

2.1 Audit Planning:

Short-term planning takes into account audit issues that will be covered during the year, whereas long-term planning relates to audit plans that will take into account risk-related issues regarding changes in the organization's IT strategic direction that affect the organization's IT environment.

To perform audit planning, the following steps are to be followed in order:

- Gain an understanding of the business's mission, objectives, purpose and processes, which include information and processing requirements, such as availability, integrity, security and business technology.
- Identify stated contents such as policies, standards and required guidelines and organization structure.
- Evaluate risk assessment (If applicable).
- Perform a risk analysis (If applicable).
- Conduct an internal control review.
- Set the audit scope and audit objectives.
- Develop the audit approach or audit strategy.
- To be developed and document a risk-based audit approach (if applicable)
- To develop an audit program and procedures.

2.2 Performance of Audit Work

Evidence

During the course of the audit; sufficient, reliable and relevant evidence shall obtain to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

Documentation

The audit process should be documented, describing the audit work performed and the audit evidence that supports findings and conclusions.

2.3 Reporting

- The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.
- The report should state the findings, conclusions and recommendations and any reservations, limitations in scope with respect to the audit.
- Sufficient and appropriate audit evidence to be obtained to support the reported results.

2.4 Using the Work of Other Experts

- The IT auditor should, where appropriate, consider using the work of other experts for the audit.
- The IT auditor should assess, review and evaluate the work of other experts as part of the audit and conclude the extent of use and reliance on expert's work.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
2	**IT Auditing Procedures**	December 2016	-

2.5 Audit Evidence

It is imperative to obtain sufficient and appropriate audit evidence to draw reasonable conclusions on the audit results. It is also necessary to evaluate the sufficiency of audit evidence obtained during the audit

Audit evidence shall include the following:

- Includes the procedures as performed by the auditor
- Includes source documents (in either electronic or paper format), records and corroborating information used to support the audit

2.6 Communicating Audit Results

Before communicating the results of an audit to senior management, the findings should discuss with the management staff of the audited entity. The goal of such a discussion would be to gain agreement on the findings and to develop a course of corrective action.

2.7 Audit Report Structure and Contents

There is no specific format for IT audit report. Audit reports, however, usually will have the following structure and content:

2.7.1 An introduction to the report, including a statement of audit objectives and scope, the period of audit coverage and a general statement on the nature and extent of audit procedures examined during the audit.

2.7.2 Overall conclusion and opinion on the adequacy of controls and procedures examined during the audit.

2.7.3 Detailed audit findings and recommendations and the decision to include or not include findings in an audit report.

2.7.4 Limitations to audit

2.8 Audit Documentation:

Documentation should include, at a minimum, a record of:

- Review of previous audit documentation
- Minutes of management review meetings, audit committee meetings and other audit-related meetings (if applicable)
- The audit programme and audit procedures that will satisfy the audit objectives
- The audit findings, conclusions and recommendations
- Any report issued as a result of the audit work
- Supervisory review

2.9 Follow-up Activities

After the reporting of findings and recommendations, the IT auditor should follow -up whether appropriate action has been taken by the management in a timely manner.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	December 2016	-

Chapter: 3
IT Management

Introduction:

IT Management must ensure that the IT functions are efficiently and effectively managed. **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.

3.1 IT Policy :

Objective:

It establishes general requirements and responsibilities for protecting IT systems. 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 shall ensure management direction and support for information security in accordance with business requirement and relevant laws and regulations.

S/N	Title of the Control	Brief description of the Control
3.1.1	Information Technology (IT) Policy	The 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. The policy will require regular updates to cope with the evolving changes in the IT environment both within the bank and overall industry.
3.1.2	Information Security Policy Document	An information security policy shall be approved by management and published and communicated to all employees and relevant external parties.
3.1.3	Review of Information Security Policy Document	The Information Security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

3.2 Documentation:

Objective:

To establish an acceptable level of direction in all IT related matters at Head office level as well as compliance of Bangladesh bank directives the bank shall meticulously maintain the proper documentation for the following control.

S/N	Title of the Control	Brief description of the Control
3.2.1	Organogram	There shall be an organogram chart for IT department of the bank.
3.2.2	Job description	There shall be detailed job description (JD) which described the duties and

		responsibilities of individuals within IT department

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
3.2.3	Scheduled for roster IT operational Support	There shall be scheduled roster for IT operation
3.2.4	Segregation of duties for IT tasks	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Application development and support should not be carried out by the same person.
3.2.5	Contingency plan	Fallback plans for various levels of system support personnel

3.3 Internal IT Audit:

Objective:

The Bank is required to ensure regulatory compliance at all levels; therefore, IT Audit is aimed at ensuring an acceptable standard for security on all The City Bank's servers, workstations, routers, switches, and other IT systems. Additionally, it should ensure that proper purchase and approval procedure are followed, the documentations are correct and the inventory reflects actual approved purchase.

S/N	Title of the Control	Brief description of the Control
3.3.1	Staffing for IT Audit	Internal Audit should have sufficient IT expertise / resources capable of conducting IT Audit
3.3.2	Frequency of Internal Auditing	Internal IT audit should be conducted as per the IT Audit plan. The report shall be preserved for inspection of Bangladesh Bank officials as ready reference.
3.3.3	Compliance of internal audit report	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 3.3.2

3.4 Training:

Objective:

- The Bank recognizes the value and importance of providing opportunities to all its staff, to develop their job-related knowledge and skills, and expects that with development and training individual effectiveness will increase and they will make a richer contribution to the work of their respective division of Head Office/ Sales & Service Centers of the bank.
- It shall be the banks' policy to provide sufficient development and training to ensure the implementation of bank's IT policies designed to meet its obligations as an employer.

- It shall be the bank's policy to provide and support further development and training when required to maintain and enhance the standards of performance over a period of time.
- The objectives of designing the training policy/ program are to bridge the gap between present level of competence and desired level of competence of human resources/staffs of the bank.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
3.4.1	On the job training	Related employees should be given adequate training on sensitive IT Tasks
3.4.2	Awareness on IT security for the employees	The employees should be trained on aspects of importance and awareness of IT
3.4.3	Training for Network users'	All the network users are trained about its operating and security procedures

3.5 **Insurance:**

Objective:
To minimize the loss and/or damage of the hardware assets related to IT.

S/N	Title of the Control	Brief description of the Control
3.5.1	IT Assets insurance policy	Adequate insurance coverage should be provided under the bank's insurance policies so that costs of loss and/or damage the hardware assets related to IT are minimized

3.6 Organization of Information Security

3.6.1 Internal Organization

Objective:
To manage information security within the organization.

S/N	Title of the Control	Brief description of the Control
3.6.1.1	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information securities responsibilities.
3.6.1.2	Information Security co-ordination	Information security activities shall be co-ordinated by representative from parts of the organization with relevant roles and job functions.
3.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.
3.6.1.4	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
3.6.1.5	Independent review of information security	The organization's approach to managing information security and

		its implementation (i.e. Controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	**July 2009**	-

3.6.2 External Parties

Objective:

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

S/N	Title of the Control	Brief description of the Control
3.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
3.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
3.6.2.3	Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

3.7 Problem Management:

Objective:

The goal of 'Problem Management' is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

S/N	Title of the Control	Brief description of the Control
3.7.1	Log problem in daily/weekly basis	The IT Help Desk and other staff of IT Division should normally receive the problem from Sales and Service Centers along with Head office Division and accordingly record the problems/request into the Helpdesk software for tracking and reporting purposes, including those that are resolved on the spot. They should also set priorities among the problems as per the bank's **Problem Priority Procedure (if any).** There shall be a procedure in place to analyze the problems, their frequency, recurring

		reasons, unresolved problems and reasons there of.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
3.7.2	Problem Management Process	There shall be preventive maintenance schedule for the critical Servers/Communication to minimize problems and frequency and impact of performance failure. The Problem Management process should have both reactive and proactive aspects. The reactive aspect is concerned with solving Problems in a timely manner to minimize any negative impact on the business. Proactive Problem Management is concerned with identifying and solving Problems before incidents can even occur.
3.7.3	Accept responsibility for problem resolution, and assign the problem internally to a team member for action	IT help desk should accept responsibility for preliminary problem resolution and shall refer the reported problem/ requests that are considered higher in Priority and non-routine to the concern technical team of IT Division. After that the team leader of the concern technical team used to assign appropriate IT personnel to resolve the problem.
3.7.4	Investigate the problem report	All units of IT Division shall be logged into the Help desk software for reported problems/request and prioritized immediately. All units should usually provide spot solution over telephones for the problems or requests which are commonly dealt with on a day to day basis and as per emergency requirements some solutions are provided by physical presence with maintaining necessary documentation while supporting at remote end. Problems that do not cause immediate hazardous effects, however, repeat over a long period of time must be monitored and escalated to ensure they are resolved. However, if a problem keeps recurring, it should be brought to the attention of the Senior Problem Manger (Head of IT) to initiate investigation.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
3	**IT Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
3.7.5	Perform the necessary corrective action within the time frame bounded by the problem's severity	Necessary corrective action within the time frame used to perform by the concern officials of IT division with exercising the steps which are follows: a) In-house approach to corrective action by involving internal resources i.e. All requests should be allocated to a support group immediately for action. b) All requests should be attended to and resolved as soon as possible by IT Division. Referral to approved out-sourcing to resolve the problem within bounded time frame and considering problem's severity if corrective action failed through the step defined in the Serial number 3.7.3. Where Service Level Agreements exist, requests should be resolved within the SLA performance standards.
3.7.6	Document findings and action steps taken during the problem resolution process	IT Division should practice on the Problem Management with formal documented structured procedure and formulate action steps taken during the problem resolution process.
3.7.7	Provide remote systems problems information to specific support units and Regional Help Desk & Support Teams	IT Division of Head office shall use to provide remote support through Wide Area Network (WAN) by using Remote Desktop Connection and Virtual Network Computing (VNC) tools from Head Office. If any critical problem arises in Hardware /Network segments at remote location which could not be resolved from IT Division, Head office, in that case IT Division should handle the situation by providing skill IT personnel from Head Office.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

Chapter: 4
IT Operation Management

Introduction:

IT 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.

4.1 Change Management:

Objective:

The goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organization.

Change management is responsible for managing change process involving:

- Hardware Management
- Communications equipment and software
- System software
- All documentation and procedures associated with the running, support and maintenance of live systems.

S/N	Title of the Control	Brief description of the Control
4.1.1	Change Managements Policy	All change implemented in the production environment must be governed by a formal documented process including forms with necessary change details. A change management system may cover at minimum: 1. **General details**: Change no, Category, Approval status, Risk level, Priority, Requestor details, approver details etc 2. **Inventory**: List of resource requirement 3. **Implementation plan**: Start time, end time, Man hours 4. **Authorization**: Approved, denied ,pending, reason 5. **Change details**: Hardware/Software, Description, done by, Approved by, tested by , released by, notification , roll back plan 6. **Post implementation**: Review procedure

4.1.2	Change Management Log	Audit Logs of changes should be maintained available for ready references.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
4.1.3	User Acceptance Test (UAT)	User Acceptance Test (UAT) should be completed before change implementation. This document should be preserved for ready reference.
4.1.4	Procedure for obtaining of No Objection Certificate (NOC)	When any changes are made to the Hardware or software there shall be formal procedure of signing acceptance of the satisfactory installation and commencement of operations.

4.2 Asset Management

Objective:
The goal of asset management is to optimize asset use and manage all maintenance efforts involved in making assets as reliable, accurate, and efficient as possible.

4.2.1 Responsibility for assets:

Objective: To achieve and maintain appropriate protection of organizational assets.

S/N	Title of the Control	Brief description of the Control
4.2.1.1	Inventory of assets	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.
4.2.1.2	Disposal of IT Assets	All data on equipment and associated storage media must be destroyed or overwritten before sale, disposal or reissue. This shall be governed by a formal disposal policy.
4.2.1.3	Intellectual Property Rights (IPR issues)	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. Software license copies shall be available in the IT data vault.
4.2.1.4	SLA for Software used in production environment	Software used in production environments must be subject to a support agreement.
4.2.1.5	Restriction on usages of pirated software	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.
4.2.1.6	Ownership of assets	All information and assets associated with information processing facilities

		shall be owned' by a designated part of the organization.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	IT Operation Management	July 2009	-

S/N	Title of the Control	Brief description of the Control
4.2.1.7	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

4.2.2 **Information classification:**

S/N	Title of the Control	Brief description of the Control
5.2.2.1	Information Classification	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
5.2.2.2	Information labeling and handling	An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the bank.

4.2.3 **IT Asset Repair:**

S/N	Title of the Control	Brief description of the Control
5.2.3.1	IT Assets maintenance	Repair and maintenance records shall be reviewed periodically to analyze whether the asset repair costs exceeds cost of replacement.

4.2.4 **Human resources security**

Objective:

To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

S/N	Title of the Control	Brief description of the Control
4.2.4.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
4.2.4.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

4.2.4.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

4.2.5 Termination or change of employment

S/N	Title of the Control	Brief description of the Control
4.2.5.1	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
4.2.5.2	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

4.3 Operating Procedures:

Objective:

Standard Operating Policies and Procedures can be effective catalysts to drive performance improvement and improving organizational results.

S/N	Title of the Control	Brief description of the Control
4.3.1	Operating Procedure for IT functions	There shall be operating procedures for all IT functions facilitating by the bank.
4.3.2	Change Management Procedure for any operational changes	Changes to operating procedures must be authorized by management and documented.
4.3.3	Minimum coverage of the Operating Procedure	Operating procedures shall 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 e) Documentation on system start-up, close-down, restart and recovery
4.3.4	Annual Maintenance schedule	There shall be annual maintenance contract for the Hardware owned by the bank after the guarantee period. The bank should contemplate taking such contracts for critical hardware at the bank.
4.3.5	Schedule system maintenance	There shall be scheduled periodic preventive maintenance system for critical Hardware Assets to reduce

		frequency and impact of performance failures.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

4.4 Communications and operations management:

4.4.1 Operational procedures and responsibilities:

Objective:

To ensure the correct and secure operation of information processing facilities.

S/N	Title of the Control	Brief description of the Control
4.4.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.
4.4.1.2	Change management	Changes to information processing facilities and systems shall be controlled.
4.4.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
4.4.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.

4.4.2 System planning and acceptance:

Objective:

To minimize the risk of systems failures

S/N	Title of the Control	Brief description of the Control
4.4.2.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
4.4.2.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

4.4.3 Network security management

Objective:

To ensure the protection of information in networks and the protection of the supporting infrastructure.

S/N	Title of the Control	Brief description of the Control
4.4.3.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
4.4.3.2	Security of network services	Security features, service levels, and management requirements of all

		network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

4.4.4 **Media handling:**

Objective:

To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

S/N	Title of the Control	Brief description of the Control
4.4.4.1	Management of removable media	There shall be procedures in place for the management of removable media.
4.4.4.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.
4.4.4.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
4.4.4.4	Security of system documentation	System documentation shall be protected against unauthorized access.

4.4.5 **Exchange of information:**

Objective:

To maintain the security of information and software exchanged within an organization and with any external entity.

S/N	Title of the Control	Brief description of the Control
4.4.5.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
4.4.5.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.
4.4.5.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
4.4.5.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.
4.4.5.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
4	**IT Operation Management**	**July 2009**	-

4.4.6 **Monitoring:**

Objective:

To detect unauthorized information processing activities.

S/N	Title of the Control	Brief description of the Control
5.4.6.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.
5.4.6.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
5.4.6.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.
5.4.6.4	Administrator and operator logs	System administrator and system operator activities shall be logged.
5.4.6.5	Fault logging	Faults shall be logged, analyzed, and a appropriate action taken.
5.4.6.7	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

4.5 **Request Management:**

Objective:

In an automated system, the user submits a request through an online service catalog, and the application software automatically routes the request through the appropriate processes for approval and service delivery. These systems also typically enable users to track the status of their service requests, and management to monitor service delivery levels for quality control purposes.

S/N	Title of the Control	Brief description of the Control
4.5.1	Request Management Process	Before any IT service a formal request process must be established.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
5	**Physical and Environmental Security**	**July 2009**	-

Chapter: 5
Physical and Environmental Security

Introduction:

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.

Objective:

To prevent unauthorized physical access, damage and interference to the organization's premises and Information.

5.1 Physical Security Guideline for Tier-1

5.1.1 Data Centre Access

S/N	Title of the Control	Brief description of the Control
5.1.1.1	Restriction on Data Centre Access	Data Centre must be restricted area and unauthorized access is prohibited
5.1.1.2	Control on of data centre access	Number of entrance into the Data Centre should be limited, locked and secured.
5.1.1.3	Access Authorization procedures	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.
5.1.1.4	Maintenance of access authorization list	Bank should maintain Access Authorization list, documenting individuals who are authorized to access the data centre, reviewed and updated periodically.
5.1.1.5	Maintenance of access log	Access log with date and time, should be maintained documenting individuals who have accessed the data centre.
5.1.1.6	Visitor Log register	Visitor Log should exist and need to be maintained.
5.1.1.7	Emergency exit door	There should be Emergency exit door available in the data centre

5.1.2 Secure areas:

Objective:

To prevent unauthorized physical access, damage and interference to the organization's premises and information

S/N	Title of the Control	Brief description of the Control

5.1.2.1	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
5	**Physical and Environmental Security**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
5.1.2.2	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.
5.1.2.3	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

5.1.3 **Equipment Security:**

Objective:

To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

S/N	Title of the Control	Brief description of the Control
5.1.3.1	Equipment sitting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
5.1.3.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
5.1.3.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage
5.1.3.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.
5.1.3.5	Security of equipment off premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
5.1.3.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
5.1.3.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.

5.1.4 Environmental

Objective:

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.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Physical and Environmental Security**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
5.1.4.1	Physical layout of the data centre	Sufficient documentation is required regarding the physical layout of the data centre
5.1.4.2	Layout of power supplies and Network connectivity of the data center	Documentation regarding the layout of power supplies of the data centers and network connectivity to be prepared
5.1.4.3	Floor pattern of Data Centre	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.
5.1.4.4	Water detection device	Water detection devices should be below the raised floor, if it is raised.
5.1.4.5	Security of data centre	Existence of Closed Circuit Television (CCTVs) camera is required and to be monitored
5.1.4.6	Availability of contact information of vendors, IT personnel etc.	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.
5.1.4.7	Load balancing of Electrical outlets/ channels	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.
5.1.4.8	Data center sub-systems controls	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

Chapter No.	Chapter Name	Chapter Issued	Page Revised
5	**Physical and Environmental Security**	**July 2009**	-

5.1.5 Fire Prevention:

S/N	Title of the Control	Brief description of the Control
5.1.5.1	Fire prevention	The Data Centre wall/ceiling/door should be fire resistant.
5.1.5.2	Fire suppression system	Fire suppression equipment should be installed.
5.1.5.3	Fire alarm	Procedures must exist for giving the immediate alarm of a fire, and reporting the fire services and to be periodically tested.
5.1.5.4	Fire detection system	There should be Fire detector below the raised floor, if it is raised.
5.1.5.5	Electrification system	Electric cables in the Data Centre must maintain a quality and concealed.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

Chapter: 6
Information Security Standard

Objective:

The objective of this chapter is to specify Information Security Policies and Standard to be adopted by the City Bank Limited 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.

6.1 Access Control for information systems

6.1.1 Password Control:

Objective:

To ensure authorized user access and to prevent unauthorized access to information systems.

S/N	Title of the Control	Brief description of the Control
6.1.1.1	Password buildup procedure	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).
6.1.1.2	Creation of New user Id	When a new user ID is created; the creator and the acceptor of the user-ids should sign and formally confirm the creation and the acceptance of the user-id.
6.1.1.3	Modification of an Account's privilege	Modification to an existing account rights shall be under the custodian of dual authentication.
6.1.1.4	Password expire policy	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). Passwords in the operating systems have to be set to expire. The policy of the bank required that passwords be changed every 30 days.
6.1.1.5	Access violations of critical business systems	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).

6.1.1.6	Rules for management of passwords	Password history maintenance shall be enabled in the system to allow same passwords can be used again after at least 4 times. Password entries must be masked.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
6.1.1.7	Sensitive Password preservation policy	Sensitive passwords have to be preserved in a sealed envelope with movement records for usage in case of emergency.
6.1.1.8	Inactivation of user ID	When a Finacle user is absent for a long period the practice of making the user-id must be inactivated.
6.1.1.9	Review of Administrative password	The administrative password of the operating system shall be changed regularly. The passwords shall follow the password policy of the bank.
6.1.1.10	Sharing of security of password	There should be control that at any circumstance no user shall share his password with others. A process of vigilance should be set up to ensure sudden checking to discourage such type of usages.
6.1.1.11	Password policy for router	Router password shall be governed by the password policy of the bank. Periodic changing of password shall be done.

User ID Maintenance:

S/N	Title of the Control	Brief description of the Control
6.1.2.1	Policy on standardized naming convention for User ID	Each user must have a unique UserID and a valid password. There shall be standard naming convention being followed at the bank.
6.1.2.2	Access violations of critical business systems	The UserID shall be locked up after 3 unsuccessful log in attempts.
6.1.2.3	Rules for management of User ID & passwords	There need to have a control to ensure that user ID and password are not same.
6.1.2.4	User ID Request / Maintenance Form	The UserID Maintenance Form with access privileges shall be duly approved by the appropriate authority.
6.1.2.5	Procedure for review of access privileges	Access privileges are changed/locked within 24 hours when users' status changed or left the bank.
6.1.2.6	Maintenance of Oracle generic user id	Oracle generic user ids like system ad sys shall not be used by the Database administrators. A separate user id has to be created in their own name. There shall be dual control system for the user id like system and sys.

6.1.2.7	Assigning of Super user in the System	There shall be formal documentation of the super user level being assigned to the designated persons.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

6.2 **Network/Internet Security:**

Objective:

To protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together.

S/N	Title of the Control	Brief description of the Control
6.2.1	Documentation on Network design	The Network Design and its security shall be documented. There should be a policy on Network Access i.e. LAN, VPN and Router.
6.2.2	Physical security for the network equipment	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
6.2.3	Security control for sensitive information	The sensitive information should be kept in restricted area in the networking environment.
6.2.4	Control for electronic tempering	Unauthorized access and Electronic tampering is to be controlled strictly.
6.2.5	Security of Network administration	Security of the network should be under dual administrative control.
6.2.6	Network Firewalls	Firewalls are in place on the network for any external connectivity.
6.2.7	Redundant communication links	Redundant communication links are used for WAN.
6.2.8	Availability of Intruder detection system	There should be a system to detect the unauthorized intruder for network.
6.2.9	Data Encryption technology	There is mechanism in place to encrypt and decrypt the highly sensitive data traveling through WAN or public network.
6.2.10	Internet and e-mail policy	There shall be a policy on internet usage policy and on the usage of electronic mail.
6.2.11	Internet	All Internet connections should be routed through a Firewall for PCs connected to network.
6.2.12	Patch update of Internet browser	Microsoft updates shall be available at the banks' Intranet home page in downloadable format for all the users.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

6.3 **Virus Protection:**

Objective:

To identify, neutralize or eliminate malicious software and to combat a wide range of threats, including worms, phishing attacks, Trojans often described collectively as malware.

S/N	Title of the Control	Brief description of the Control
6.3.1	Anti Virus deployment Policy	There should be Anti-Virus installed in each server and computer whether it is connected to LAN or not.
6.3.2	Monitoring of Anti Virus Software	The anti virus software shall always be updated with the latest virus definition file.
6.3.3	Users' training on computer virus	All users shall be well-trained and informed about computer viruses and their prevention mechanism.
6.3.4	Procedure for incoming e-mail scanning	There shall be 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.
6.3.5	Firewall for internet connection	All Internet connections should be routed through a Firewall for PCs connected to network
6.3.6	Uses of Flash Drive	There should be a policy on usage of USB flash drive.
6.3.7	Update of New vulnerability	There should be a system in place to keep regular update of new vulnerabilities in the environment.
6.3.8	Update of Operating System patches	Patches of the various operating systems i.e. Windows, Sun Solaris should be updated regularly.
6.3.9	Checking of Data in Back-up cartridges	Data in the back-up cartridges are to be verified to be virus free.

6.4 Access control:

6.4.1 Business requirement for access control

Objective:

To control access to information

S/N	Title of the Control	Brief description of the Control
6.4.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access. The IT Job functions to be defined and mapped with Finacle Core banking privileges.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

6.4.2 User access management

Objective:

To ensure authorized user access and to prevent unauthorized access to information systems.

S/N	Title of the Control	Brief description of the Control
6.4.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
6.4.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.
6.4.2.3	User password management	The allocation of passwords shall be controlled through a formal management process
6.4.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process. There should be a control mechanism to check whether the user has been reset to the original privileges when the requirement of job of higher privileges is over.
6.4.2.5	Procedure for assigning of higher privilege	Documentation in the form of Request Form shall be maintained by the bank to allocate higher privilege assignments to the users'.
6.4.2.6	Access to Financial transaction	There shall be controlled that Database administrator can not access to transaction data.

6.4.3 Network access control:

Objective:

To prevent unauthorized access to networked services.

S/N	Title of the Control	Brief description of the Control
6.4.3.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.
6.4.3.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.
6.4.3.3	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

6.4.3.4	Documentation for Router configuration	Authorization of changes to router configuration shall be documented. Changes in the router configuration shall also be documented.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	**-**

6.4.4 Operating system access control

Objective:

To prevent unauthorized access to operating systems.

S/N	Title of the Control	Brief description of the Control
6.4.4.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.
6.4.4.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
6.4.4.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.
6.4.4.4	Session time-out	Inactive sessions shall shut down after a defined period of inactivity.
6.4.4.5	Limitation of connection time	There shall be restriction on connection time for banking application. Restrictions on connection times shall be used to provide additional security for high-risk applications.
6.4.4.6	Operating hour for the users	Operating time schedule for the users is to be defined where necessary.
6.4.4.7	Terminal inactivation policy	The terminal inactive time allowable for users should be set in accordance with the Bank's policy. Restriction shall be imposed on the use of account /terminal after the normal business hour.

6.4.5 Application and information access control

Objective:

To prevent unauthorized access to information held in application systems.

S/N	Title of the Control	Brief description of the Control
6.4.5.1	Information Access policy	There shall be acceptable usage policy in the bank. This policy should detail the purpose for which the information and information assets of the bank may be used, the information that may be shared and the personnel who may do so.
6.4.5.2	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.

6.4.5.3	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.
6.4.5.4	Access log for operating system	Security Logs for access to the operating system shall be enabled and reviewed periodically.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
6.4.5.5	Maintain of access log for Oracle database	There shall be recorded of all access by the Database Administrator to the Oracle Database which shall be reviewed by the authorized personnel periodically.
6.4.5.6	Monitoring of Finacle Access Log	There shall be a procedure in place for review of the Finacle Access log (Login, Logout, Tempering of the users etc.) for monitoring the information processing facilities to ensure whether users are performing activities that are explicitly authorized.
6.4.5.7	Monitoring of Finacle Access Log for usage of privilege accounts	Logs for usage of privilege accounts and their review by an independent person shall be reviewed.
6.4.5.8	Logs for remote access	Remote access from IT division at branch level shall be recorded in a log register. Why the access was required and what was done on making such access and records of the person making the access shall be maintained.
6.4.5.9	Access log for Router	Periodic review of access logs of the router shall be maintained.

6.5 Information systems acquisition, development and maintenance

6.5.1 Application development

Objective:

To ensure all the relevant procedures of System Development Life Cycle and documentation while developing an Application either by the third party or in- house software development.

S/N	Title of the Control	Brief description of the Control
6.5.1.1	Policy on Application Development	There shall be formal policy on the framework of software development which should include feasibility study methodology, testing methodology, parallel run requirements and final roll out of the software. There should be a standardized organizational System Development Life Cycle (SDLC).
6.5.1.2	Change Management Procedure	Change Management documentation shall be maintained while changes made to the original requirement specification documentation. Change authorization, approval

		documentation and program testing are to be formally documented.
6.5.1.3	Procedure for modification of Software	The developer shall maintain proper documentation for any modifications of programs.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
6.5.1.4	Version control	There shall be formal system of maintaining a program library and version control. A version control system shall be in place for in-house developed software.
6.5.1.5	Maintain of history records of code check-in/out and deletions.	The history records of code check-in/out and deletions shall be maintained by the in-house developer and 3rd party developer.
6.5.1.6	Logic flow diagram for development of any application software	Logic flow diagram of a solution prior to coding any application software required by the bank.
6.5.1.7	Controls for outsourced software	There shall be standardized controls for outsourced software e.g. the licensing arrangement, escrow arrangement, contractual requirement for quality assurance , testing before installation etc.
6.5.1.8	Preservation of source code	Source code shall be frozen and the development team should discontinue the development activities after the software moves into the production environment.

6.5.2 **Security requirements of information systems**

Objective:

To ensure that security is an integral part of information systems.

S/N	Title of the Control	Brief description of the Control
6.5.2.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

6.5.3 **Correct processing in applications**

Objective:

To prevent errors, loss, unauthorized modification or misuse of information in applications.

S/N	Title of the Control	Brief description of the Control
6.5.3.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.
6.5.3.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts

6.5.3.3	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
6	**Information Security Standard**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
6.5.3.4	Dual Authentication System	The software should not allow the same person to be both the maker and checker of the same transaction.

6.5.4 **Security in development and support processes**

S/N	Title of the Control	Brief description of the Control
6.5.4.1	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.
6.5.4.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
6.5.4.3	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.

6.6 Information security incident management

6.6.1 Reporting information security events and weaknesses:

Objective:

To ensure information security events and weaknesses associated with information systems are communicated in a man

S/N	Title of the Control	Brief description of the Control
6.6.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
6.6.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
7	System Software Controls	July 2009	-

Chapter: 7
System Software Controls

7.1 Controls on Internet Banking

Objective:

Internet banking refers to the use of the Internet as a remote delivery channel for banking services. Services include such as cheque book inquiry, inquiry of account balance, account summary, printing of bank statement, view all standing instructions and other banking services, such as utility bill payments.

S/N	Title of the Control	Brief description of the Control
7.1.1	Policy on Internet Banking	There shall be policy regarding the customers' authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs, legal issues associated with Internet banking.
7.1.2	Change Control Procedures	There shall be appropriate procedures in place regarding change control, review of audit trails and the review/analysis of usage logs (firewall logs and other reports).
7.1.3	Regularity compliance for data integrity	There shall be suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice.
7.1.4	Intrusion Detection and Prevention Systems	There shall be procedure in place for Intrusion detection systems and virus control systems.
7.1.5	Firewall Technology	The communication across the network shall be made secure using virtual private network (VPN) and related encryption techniques are in placed.
7.1.6	Data Encryption Technology	Adequate and strong encryption algorithms shall be placed to protect data during communication across the network.
7.1.7	Review of business continuity and contingency plans of third-party service providers	The bank has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers.
7.1.8	Business continuity and contingency plans for critical Internet banking processing	There shall be in place appropriate business continuity and contingency plans for critical Internet banking processing and/or delivery systems and regularly tested, and whether the

		bank receives copies of test result reports.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
7	System Software Controls	July 2009	-

S/N	Title of the Control	Brief description of the Control
7.1.9	Physical security of IT Assets of Internet banking	There shall be adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system.
7.1.10	Maintenance of transaction records	There shall be record for customer transaction, transaction number, transaction type, transaction amount and other information of relevance for control purposes.

7.2 Parameter settings:

S/N	Title of the Control	Brief description of the Control
7.2.1	Change control process for parameter settings	There shall be procedure in place for documenting change of parameters, the person changing the same and the reasons for such changing.
7.2.2	Non financial report printing parameters	Non financial report printing parameters in Finacle shall be enabled for generating reports on password changing date, password expiry date etc.

7.3 Transaction Processing & System Software Controls:

S/N	Title of the Control	Brief description of the Control
7.3.1	Automated process for premature FDR encashment	Review whether calculation of interest for premature encashment of Fixed Deposit Receipt (FDR) account is processed by automated system
7.3.2	Validation of DD/PO/Pay slip	To verify that DD/PO/Pay slip is validated by the checker after it has been issued by the maker
7.3.3	Review of modification of any record in the system	Review of system generated log report of modifications made to the master files or any modification of any record in the system
7.3.4	Review of exceptional log report	Review of exceptional log report (if any)
7.3.5	Review of validation report	Review the list of records which are not validated on due course
7.3.6	Review of system generated report for new accounts to ensure regularity requirements	System generated report for opening of new accounts to ensure that all regularity requirement are complied
7.3.7	Audit trail	Review of System generated Log report/Audit trail. Review of un-successful attempts in the system.
7.3.8	Review of System Software controls/functionalities	ICCD can review any controls/functional area of the

		Banking software as and when required.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
8	**Business Continuity and Disaster Recovery Management**	**July 2009**	-

Chapter: 8
Business Continuity and Disaster Recovery Management

Introduction:

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. The purpose of the BCP is to identify and reduce risks, limit the consequences if a damaging incidents occur, and ensure the timely resumption of essential operations.

8.1 Business Continuity Plan (BCP):

Objective:

The objectives of a business continuity plan (BCP) are to minimize financial loss to the institution; continue to serve customers and financial market participants; and mitigate the negative effects disruptions can have on an institution's strategic plans, reputation, operations, market position, and ability to remain in compliance with applicable laws and regulations. BCP is required to cover operational risks and should take into account the potential for wide area disaster, data centre disaster and the recovery plan. The development of a BCP Instruction Manual should have five main phases:

1. Business Impact Analysis (BIA)
2. Solution design
3. Implementation
4. Testing and acceptance
5. Maintenance.

S/N	Title of the Control	Brief description of the Control
8.1.1	Policy on Business Continuity	There must be a Business Continuity Plan (in line with business) for IT in place.
8.1.2	Preservation of Business continuity documentation	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 Head office for ready reference.
8.1.3	Key issues regarding BCP	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

8.1.4	Frequency of review of BCP	Review of BCP must be done at least once a year

Chapter No.	Chapter Name	Chapter Issued	Page Revised
8	**Business Continuity and Disaster Recovery Management**	**July 2009**	-

8.2 Information security aspects of business continuity management

Objective:

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

S/N	Title of the Control	Brief description of the Control
8.2.1	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information Security requirements needed for the organization's business continuity.
8.2.2	Business continuity and risk assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
8.2.3	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
8.2.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
8.2.5	Testing, maintaining and reassessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

8.3 Disaster Recovery Plan (DRP):

Objective:

The purpose of the Disaster Recovery plan is to establish the rules for recovering data in case of any disaster with in a minimum down time.

S/N	Title of the Control	Brief description of the Control
8.3.1	Policy on DR	A Disaster Recovery Site (DRS) must be in place replicating the Data Center (Production Site).
8.3.2	Distance of DR site from production site	DR site must be at a minimum of 10 kilometers (radius) of distance from the 'production' site.

8.3.3	Hardware & telecommunication requirement for DR site	DR site is equipped with compatible hardware and telecommunications equipment to support the live systems in the event of a disaster.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
8	**Business Continuity and Disaster Recovery Management**	**July 2009**	-

S/N	Title of the Control	Brief description of the Control
8.3.4	Off-site preservation of up-to-date DR plan	An up-to-date and tested copy of the DR plan is securely held off-site. DR plans exist for all the critical services where DR requirement is agreed with the business.
8.3.5	Frequency of DR testing	DR test is successfully carried out at least once a year.
8.3.6	UAT on DR documentation	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

8.4 **Backup:**

Objective:

Backup of data in an external media is necessary so that data from external media can be restored in the following situations:

1. Database corrupts
2. Data store device such as hard disks fails
3. Some data in the database corrupts due to malfunctioning of a process during End of Day (EOD) or some other process.

S/N	Title of the Control	Brief description of the Control
8.4.1	Backup and restore procedure	There should be a documented back up and restore procedure mentioning who, when and how to backup and restore data. Back up Schedule of mail server shall be planned in every 6 hours as mails have financial impact.
8.4.2	Off-site preservation of data backup	Backup copies of information should transmit off-site at separate and safe environment i.e. Disaster Recovery site (DRS) with minimum time interval.
8.4.3	On-site preservation of data backup	There shall be at least one backup copy kept on-site for time critical delivery.
8.4.4	Data backup cycles	The backup cycle should be based on daily, monthly, quarterly, and Yearly.
8.4.5	Maintain of backup log sheet	The back up media shall be send off-site immediately after the back up has been taken. The back up log sheet shall be maintained, checked & signed by supervisor.
8.4.5	Verification of data backup	The ability to restore from backup media shall be tested at least

		quarterly. Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
8	**Business Continuity and Disaster Recovery Management**	**July 2009**	-

8.5 Compliance:

8.5.1 Compliance with legal requirements

Objective:

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

S/N	Title of the Control	Brief description of the Control
8.5.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
8.5.1.2	Intellectual property rights(IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
8.5.1.3	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.

8.6 Compliance with legal requirements

Objective:

To ensure compliance of systems with organizational security policies and standards.

S/N	Title of the Control	Brief description of the Control
8.6.1	Compliance with security policies and standards	All concern shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
8.6.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
9	**Service Provider Management**	**July 2009**	-

Chapter: 9
Service Provider Management

9.1 Service Level Agreement (SLA)

Objective:

The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service. It is important to note that the 'agreement' relates to the services the customer receives, and not how the service provider delivers that service.

S/N	Title of the Control	Brief description of the Control
9.1.1	Service Level Agreement (SLA)	There should be Service Level Agreement between the vendor and the bank.
9.1.2	Annual Maintenance Contact (AMC)	The Annual Maintenance Contact (AMC) with the vendor should be active and currently in force.
9.1.3	Maintenance clause for Hardware equipment	The user site should ensure that the equipment does not contain sensitive live data when hardware are taken by the vendors for servicing / repair.
9.1.4	Key Issues to be considered for Service Level Agreement (SLA).	Service Contracts with all service providers including third-party vendors should include: i. Pricing ii. Measurable service/deliverables iii. Timing/schedules, i.e. service levels iv. Confidentiality clause v. Contact person names (on daily operations and relationship levels) vi. Roles and responsibilities of contracting parties, including an escalation matrix vii. Renewal period viii. Modification clause ix. Frequency of service reporting x. Termination clause xi. Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies xii. Geographical locations covered xiii. Ownership of hardware and software xiv. Documentation to be maintained (e.g. logs of changes, records of reviewing event logs) xv. Audit rights of access (internal audit, external audit, other audit as may be appropriate xvi. Security requirement

		xvii. Disaster recovery and business continuity planning xviii. IPR Issues xix. Dispute resolution/arbitration

Chapter No.	Chapter Name	Chapter Issued	Page Revised
10	**ATM Operations**	**July 2009**	-

Chapter 10
ATM Operations

Introduction:
An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of the bank with access to financial transactions without the need of bank teller.

Objective:
Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances.

The primary information criteria most relevant to ATM operations and audit process are:

- Efficiency
- Effectiveness
- Confidentiality
- Integrity
- Availability
- Reliability
- Compliance

10.1 General controls

10.1.1 There shall be complete detailed process and control descriptions related to the ATM process.

10.1.2 Review of policies and standards related to the ATM process

10.1.3 There shall be a complete inventory of hardware, software and telecommunications protocols used to support the ATM process

10.1.4 Review the prior audit report and findings and determine the action to be taken by management

10.1.5 Review the record retention policy and determine its adequacy.

10.1.6 Review insurance coverage for ATM liability, business interruption and fidelity.

10.1.7 Review whether the terminals are insured from theft, burglary and other exposures.

10.1.8 Review whether the documented user training material is available and displayed at the point of use i.e. Intranet

10.1.9 Review whether the documentation for business continuity and disaster management plans are available

10.1.10 Review whether the Helpdesk Management Procedure is in place exclusively for Debit Card/Credit Card

10.1.11 Review procedure for Key Management i.e. Vault key, Front door key, Cash cassette key, custodian of duplicate key

10.2 Physical controls

10.2.1 Review whether the terminals are securely locked with access control mechanisms installed.

10.2.2 Review whether the terminal is accessible only by authorized persons.

10.2.3 Review whether there is restriction on the maximum number of persons in the premises at any given point of time.

10.2.4 Review whether people in the queue are NOT able to view information in the screen provided by the user.

10.2.5 Review whether there is adequate management supervision over the ATM terminal

10.2.6 There shall be a system to capture, store and retrieve an image of the user with corresponding activity details by CCTV and shall be preserved for at least 3 months.

10.2.7 CCTV recording, retention and recovery process
10.2.8 Review whether there is burglary alarm arrangement in the ATM's.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
10	**ATM Operations**	**July 2009**	-

10.2.9 Review whether there is adequate security and protection for transferring/uploading cash into the ATM and carrying cash from the Sales and Service Centers.
10.2.11 Review ATM printout slips disposal mechanism.

10.3 Process controls/Reconciliation
10.3.1 Review general ledger accounts related to ATM are reconciled on a timely basis.
10.3.2 Review whether reconciliation exceptions are reviewed and action is taken regularly.
10.3.3 Review whether documented procedures are available and current for balancing and settling transactions.

10.4 **Transmission and system failures**
10.4.1 There shall be an incident log for all interruptions to normal processing.
10.4.2 In the event of a hardware failure, determine whether processing can be switched to an alternate terminal.
10.4.3 In the event of line failure, determine whether a redundant/backup communication media is available.

10.5 System logon controls
10.5.1 Verify whether the system validates all authorized users.
10.5.2 Verify whether the system provides a record of all attempts to work outside authorized functions. If so, determine whether this record is reviewed periodically and appropriate action taken.
10.5.3 Verify whether the system provides a record of all password/logon violations and that it is reviewed regularly.
11.5.4 Verify whether the system requires the use of a secure key to validate the client as an authorized user.

10.6 PIN controls
10.6.1 Review the personal identification number (PIN) issuance procedure.
10.6.2 Verify whether PINs are adequately protected during storage and transmission.
10.6.3 Review encryption procedures on PIN storage.
10.6.4 Review procedure of PINs during delivery.
10.6.5 Review that PIN mailers are not mailed together with the customer card. The most desirable control is to send PIN and card through different service providers.
10.6.6 Review that the PIN system restricts access to a customer account after 3 number of unsuccessful access attempts.
10.6.7 Review unsuccessful logon attempts and action taken by the customer/bank
10.6.8 Review the process for forgotten PINs and issue of new PINs.

10.7 Card Operations controls
10.7.1 Review on site operational procedure of ATM i.e. Card punching, cash withdrawal, customer feed back box etc.
10.7.2 Review **card issuance** procedure, including the:
- Adequacy of control over procurement of cards
- Written agreement with the card manufacturer
- Audit report of the card manufacturer
- Controls over mailing and delivery of cards to customers

10.7.3 Review the following :
- Process for handling returned cards and lost cards
- Process of cards captured or inadvertently left at ATM terminals

Chapter No.	Chapter Name	Chapter Issued	Page Revised
10	**ATM Operations**	**July 2009**	-

10.7.4 Review **card usage**:

- Card activation
- Cards issued and not activated
- Closed accounts, dormant accounts, deceased accounts

10.7.5 Review contract with card manufacturer, quality assurance process by manufacturer, controls over non-generation of unauthorized cards by manufacturer or the employees of the manufacturer, and adequate protection due to lapse by manufacturer.

10.8 Fraud prevention:

10.8.1 Review the following to ensure a mechanism exists for prevention of fraud relating to ATM:

- ATM operation policies and procedures
- Physical security surrounding all ATM components
- Effectiveness of network operating system security
- Effectiveness of system logging
- Effectiveness of segregation of duties (maker/checker/sender)
- Reconciliations
- Usage pattern tracking (such as frequency of logins, money withdrawals, same day withdrawals) for possible money laundering or intent to commit fraud

10.9 Cash replenishment Process:

10.9.1 Review the procedure to ensure proper mechanism is in place for cash replenishment

10.9.2 Review whether the cash replenished is performed by the nearest designated branch

10.9.3 Verify the maintenance of log book for cash replenished

10.9.4 Monitoring the cash status of the ATM/Vouchering system

10.10 Transaction journal:

Determine that the transaction journal information includes the:

- Transaction type
- Transaction number
- Currency
- Amount
- Account numbers
- Originating terminal
- Time and date
- Custody of journal transactions

10.11 Audit trail:

Review the system journal and log records

10.12 **ATM Maintenance**

i. **ATM Maintenance Policy**

There shall be SLA with respective vendors for ATM maintenance.

ii. **Booth Maintenance Policy**

- Booth maintenance shall be included with the work order of ATM Booth construction.

iii. **Communication Maintenance Policy**

- There shall be a policy on maintenance of communication system maintained by IT Division of the bank.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
10	**ATM Operations**	**July 2009**	-

10.13 ATM Network monitoring tools

10.13.1 There shall be procedure in place to record the downtime and the problems relate to the ATMs or shall be analyzed by the respective divisions for such failures.

10.14 **SMS Banking Operations**

11.14.1 There shall be an operational Flow chart of SMS Banking Operations

11.14.2 There shall be Annual Maintenance Contact (AMC) with the vendor for operational support

11.14.3 There shall be Disaster Recovery Plan (DRP) for SMS Banking System

11.14.4 To Verify introduction of dual authentication system in SMS banking operations

11.14.5 There shall be Operational manual on SMS Banking Service with technical layout

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	Risk Based IT Audit	July 2009	-

Chapter 11
Risk Based IT Audit

11.1 Introduction:

Risk is the possibility of an act or event occurring that would have an adverse effect on the organization and its information systems. Risk can also be the potential threat that will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the asset.

Information Technology (IT) is integral in the financial reporting of most entities today, ranging from simplistic small business accounting systems to sophisticated, virtual software solutions. To identify the key changes in the field IT; an audit methodology is to be developed to ensure that IT-related risks are appropriately considered. By better identifying the risks of material misstatement and designing the audit procedures to address those specific risks, a higher quality and more efficient audit can be conducted.

11.2 Standards of Fieldwork:

- Gather information on the entity's environment, including internal control, to assess the risks of material misstatement
- Evaluate that information to assess risks at the assertion level
- Design and perform further audit procedures based on those risks
- Evaluate the audit evidence obtained
- Reach conclusions

The Standards of Fieldwork clarify the requirements of the auditor in relationship to the IT control environment. For example:

First Standard of Fieldwork

Requires adequate planning of the audit, which includes understanding the entity, its IT environment and IT-related internal controls

Second Standard of Fieldwork

An understanding about IT controls and may include testing of IT controls as part of further audit procedures

11.3 Objective:

Information Technology development has brought momentous transformation in the banking arena. Security of IT systems for a financial institution has gained much greater importance and it is vital to ensure that risks are properly identified and managed. Bank must take the responsibility of protecting the information from unauthorized access, modification, disclosure and destruction to protect customers' interest. In view of that, Internal Control & Compliance Division has prepared a Risk based IT Audit Guideline for the bank.

The objective of a risk model is to optimize the assignment of IT audit resources through a comprehensive understanding of the IT audit universe and risks associated with each universe item.

The primary objectives of the Guideline are:

- 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;

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	**Risk Based IT Audit**	**July 2009**	-

- ❖ Prioritize information and information systems that are to be protected;
- ❖ To ensure that security risks are cost effectively managed;
- ❖ To ensure compliance with laws and regulations;
- ❖ Identification and clarification of existing information security management processes;
- ❖ To determine the status of information security management activities;
- ❖ To determine the degree of compliance with the policies, directives and standards adopted by an organization;
- ❖ To provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons;
- ❖ Implementation of business-enabling information security and
- ❖ To provide relevant information about information security to customers.

11.4 Consideration in different steps of the risk based audit:

- ❖ Planning
- ❖ The Internal Control Environment and control procedures
- ❖ Analytical procedures in planning the audit
- ❖ Sampling and other selective testing procedures
- ❖ Sample Selection Method
- ❖ Quality Control of Audit Work
- ❖ Audit Materiality
- ❖ Relation Materiality and Audit Risk

11.5 Risk Based IT Audit Approach:

By understanding the nature of the business, identification and categorization of the types of risks that will better determine the risk model. The risk assessment model can be as simple as creating weights for the types of risks associated with the business and identifying the risk in an equation. On the other hand, risk assessment can be a system where risks have been given elaborate weights based on the nature of the business or the significance of the risk.

11.6 IT Risk Assessment Measurement Methods:

IT audit risk assessment measurement is a methodology to produce a risk model to optimize the assignment of IT audit resources through a comprehensive understanding of the organization's IT environment and the risks associated with each auditable unit. Several methods are currently employed to perform IT risk assessments. One such risk assessment approach is a **scoring system** that is useful in prioritizing IT audits based on an evaluation of risk factors that consider variables such as technical complexity, extent of system and process change and materiality.

Another form of IT risk assessment is judgmental. This entails making an independent decision based upon executive management directives, historical perspectives and business climate.

11.7 Scoring methodology:

1. **Basic Principal:** Based on the Compliance Status, Risk Rating/Grading will be assigned. High Risk for Low Grade and Low Risk for High Grade.
2. **Group Weight:** Importance or weights are assigned for each group out of 100 in consideration of the severity that exposed higher financial loss, regulatory non compliance and reputational issues.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	**Risk Based IT Audit**	**July 2009**	-

3. **Assigning the Risk Level and the counter Risk Weight for each criterion** are also assigned in consideration of the severity that exposed higher financial loss, regulatory non compliance and reputational issues.
4. **Judgment Process for each criterion like objective or subjective**: Level of Subjective Judgment and Objective Judgment should be defined.
5. **Spot rectification** will be considered 20% of Risk grading score.
6. **Based on the Final Score,** the IT-Audit Grading will be assigned in a set scale like 0.00 to 1.00 where 0.00 exposed low risk i.e. High Grading and 1.00 exposed high risk i.e. Low Grading as follows:

Overall Risk grading:

SCORE	Risk Rating	Risk Grading
0.00 - 0.05	Very Low	Excellent
0.06 - 0.10	Low	Very Good
0.11 - 0.18	Medium	Good
0.19 - 0.28	Marginal	Acceptable
0.29 - 0.40	High	Unsatisfactory
0.41 - 1.00	Very High	Poor

Risk Score for each subject matter:

(a) Risk score 1.00 =Low effectiveness = High risk ; based on qualitative judgment
(b) Risk score 0.50 = Medium effectiveness = Medium risk; based on qualitative judgment
(c) Risk score 0.25 = High effectiveness = Low risk; based on qualitative judgment.
(d) Risk score 0= No risk

Case-I

Each control area of the checklist shall carryout risk. If the control area of the checklist is found in order i.e. high effective ness; the control will carryout risk weightage 1 where highest risk weightage is 5;

Case-II

If the control area of the checklist is medium effectiveness; the control area will carryout risk weightage 3 where highest risk weightage is 5.

Case-III

If the control area of the checklist is low effectiveness; the control area will carryout risk weightage 5.

Any other matter which the auditor feels necessary at the time of Audit should be pointed out according to the weight age of risk and financial gravity:

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	**Risk Based IT Audit**	**July 2009**	-

11.8 Procedural Guidelines Risk based Internal IT Audit

Step 01: Identification of risk on the basis of IT Audit Guideline and Checklist for conducting IT audit; which will be reviewed by the bank time to time as per changes of IT infrastructure of the Bank.

Step 02: Source documents to be audited

- All papers/records/documents/ledger/ system available in the Head Office Division and Sales & Service Centers.
- IT Guideline, IT Circulars, IT Manuals, Process flow, shall be preserved by the Sales & Service Centre and Head Office Divisions on each & every control functions/elements/sub-elements.

Step 03: Working steps for risk assessment of each individual auditable activities:

- Determine Sampling size
- Basis of sampling
- Walk Through test on individual activity
- Test of Control
- Control measure as per IT Audit guideline and its compliance by the Head office Divisions and Sales & Service Centers.
- Obtain the result of item wise control effectiveness of risk score from control effectiveness of risks categorically (as per gravity of the risk) by applying auditor judgment.
- Score
- Conclusion.

Step 04: **Determination of over all Internal Control Status and its effectiveness**

Based upon the ultimate assessed risk score; all Sales & Service Centers of the banks overall risk status will be determined finally by ICC Division

Steps 05: Collection of Data:

Information describing all aspects of the organization's operation will be used to define the various auditable units and to model the IT risks inherent in the unit's operations. Sources of this data shall include:

- Recent review reports
- The IT strategic plan
- Issues raised by the external auditors
- IT audit knowledge and awareness of significant issues gathered from any other sources

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	**Risk Based IT Audit**	**July 2009**	-

11.9 Audit Materiality

11.9.1 Audit Evidence Requirement:

It is very imperative to use the most appropriate, reliable and sufficient audit evidence attainable and consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.

The various types of audit evidence that should consider include the following:

- Observed processes and existence of physical items
- Documentary audit evidence
- Representations
- Analysis

Observed processes and existence of physical items can include observations of activities, property and IT functions, such as:

- An inventory of media in an offsite storage location
- Data centre/ communication room security system in operation

Documentary audit evidence, recorded on paper or other media, can include:

- Results of data extractions
- Records of transactions
- Program listings
- Invoices
- Activity and control logs
- System development documentation

Representations of those being audited can be audit evidence, such as:

- Written policies and procedures
- System flowcharts
- Written or oral statements

11.9.2 Audit Documentation:

Documentation should include, at a minimum, a record of:

- Review of previous audit documentation
- The planning and preparation of the audit scope and objectives. It is vital to have an understanding of the industry, business domain, business process, product, vendor support and overall environment.
- Minutes of management review meetings, audit committee meetings and other audit-related meetings (if applicable)
- The audit programme and audit procedures that will satisfy the audit objectives
- The audit steps performed and audit evidence gathered to evaluate the strengths and weakness of controls
- The audit findings, conclusions and recommendations
- Any report issued as a result of the audit work
- Supervisory review

11.9.3 Audit Sampling:

Audit sampling is defined as the application of audit procedures to less than 100% of the population to evaluate audit evidence about some characteristic of the items selected in order to form or assist in forming a conclusion concerning the population.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
11	**Risk Based IT Audit**	**July 2009**	-

When using either statistical or non-statistical sampling methods, it should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient, reliable and relevant audit evidence.

When designing the size and structure of an audit sample, it is to be considered the specific audit objectives, the nature of the population and the sampling and selection methods.

Method of sampling selection:

i. **Random sampling**

Ensures that all combinations of sampling units in the population have an equal chance of selection

For example:

Page	Line
5	5
20	15
23	22
29	29

Interval sampling:

For example:

First item	Second item	Third item	Etc.
39	189	339	(last item + 150)
66	216	366	(last item + 150)
91	241	391	(last item + 150)

ii. Systematic sampling

Involves selecting sampling units using a fixed interval between selections, the first interval having a random start.

iii. **Haphazard sampling**

In which sample is selected without following a structured technique, however avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population

iv. **Judgmental sampling**

Judgmental sampling involves selecting sample items based on the auditor's personnel reasoning or suspicions, in which a bias is placed on the sample. It should be noted that a judgmental sample is not statistically based and results should not be extrapolated over the population as the sample is unlikely to be representative of the population.

Chapter No.	Chapter Name	Chapter Issued	Page Revised
12	**References**	**July 2009**	-

Chapter 12
References

12.1 **Reference:**

The Control objective and control are derived from **ISO** (the International Organization for `Standardization) and **IEC** (the International Electro technical Commission) **17799:2005**, **"Guideline on Information & Communication Technology for Scheduled Banks and Financial Institutions"** of Bangladesh Bank, **Information System Audit and Control Association (ISACA) Guidelines** and Information System Audit Report conducted by Arif Ahmed & Associates, Chartered Accountants, Kolkata, India.

12.2 **Review of IT Audit Guidelines:**

The **Control and controls objective** which are furnished in the guidelines are not exhaustive and the bank may consider additional controls at the time of conducting audit as per the qualitative judgment of the auditor as well as changes of IT infrastructure of the bank.

The **IT Audit Guidelines** may be reviewed by the bank at least once in every year with the changes of IT infrastructure of the bank.