उत्तर प्रदेश ग्रामीण बैंक
Uttar Pradesh Gramin Bank

प्र.का./01/निरी./2025-26/परिपत्र/21

दिनांक: 01.05.2025

उत्तर प्रदेश ग्रामीण बैंक की सभी शाखाओं एवं कार्यालयों हेतु परिपत्र
अंकेक्षण एवं निरीक्षण विभाग द्वारा जारी

महोदय/महोदया,

विषय: *"Information System Audit Policy (Version – 1.0)" का क्रियान्वयन*

भारत सरकार के दिनांक 07 अप्रैल 2025 के राजपत्र अधिसूचना CG-DL-E-07042025-262329 (F. No. 7/6/2024/ (11)-RRB) के अनुसार, पूर्ववर्ती बड़ौदा यू.पी. बैंक, पूर्ववर्ती आर्यावर्त बैंक एवं पूर्ववर्ती प्रथमा यू.पी. ग्रामीण बैंक के समामेलन के फलस्वरूप 01.05.2025 से "**उत्तर प्रदेश ग्रामीण बैंक**" अस्तित्व में है। नवगठित बैंक में एकरूपता, पारदर्शिता और परिचालन दक्षता सुनिश्चित करने के लिए मौजूदा नीतियों को एकीकृत कर "***Information System Audit Policy (Version – 1.0)***" को बैंक की Steering Committee द्वारा मंजूरी दी गई है एवं **उत्तर प्रदेश ग्रामीण बैंक** हेतु तत्काल प्रभाव से लागू करने का निर्णय लिया गया है।

Information System Audit Policy (Version – 1.0) में समाहित बिन्दुओं /मार्गदर्शी प्रक्रियाओं पर पूर्ववर्ती बैंकों में पूर्व निर्गत निर्देश तदनुसार संशोधित माने जाएंगे|

सभी शाखाएं /कार्यालय इस परिपत्र की विषय वस्तु को भली भांति समझ लेवें एवं तदनुसार कार्य करते हुए शत-प्रतिशत अनुपालन सुनिश्चित करें|

भवदीय

(घनश्याम सिंह)
महाप्रबन्धक

संलग्नक: ***Information System Audit Policy (Version – 1.0)***

प्रधान कार्यालय: द्वितीय एवं तृतीय तल, एनबीसीसी कमर्शियल कॉम्प्लेक्स, वरदान खंड, गोमती नगर एक्सटेंशन, लखनऊ - 226010
Head Office: 2nd and 3rd floor, NBCC Commercial Complex, Vardan Khand, Gomti Nagar Extension, Lucknow - 226010
email- ho@barodauprrb.co.in

Information System Audit Policy
(Version – 1.0)

Uttar Pradesh Gramin Bank
Audit & Inspection Department
Head Office, Lucknow

Uttar Pradesh Gramin Bank

Information System Audit Policy (Version 1.o)

Document Name	Information System Audit Policy
Document ID	Information System Audit Policy
Document Owner	General Manager (Audit dept.)
Document Version No.	1.o
Document Version Date	
Prepared By	Audit and Inspection Department
Reviewed By	
Approved By	

Document Information

Version History

Version No.	Version Date	Revised by
1.o		

Current Version Reviewed by

Version No.	Designation
1.o	

Distribution List

Version No.	Name	Designation	Department
1.o	N.A.	All Departmental Heads and Heads of Controlling Offices.	All Departments, Controlling Offices and Branches

उत्तर प्रदेश ग्रामीण बैंक
UTTAR PRADESH GRAMIN BANK

Uttar Pradesh Gramin Bank

Information System Audit Policy (Version 1.o)

Document Information

Table of Contents

Information System Audit Policy

Introduction

Technology adoption by Banks and Financial Institutions has increased significantly in recent times and technological innovation has become the key tool to drive the financial services to the unreached population. In order to maintain transparency and safety in delivering the banking and other financial services to the rural mass and also to mitigate the risks emanating from adoption of technology, there is imperative need for introduction of Information Systems Audit (I.S. Audit) in the Rural Financial Institutions like RRBs.

In the wake of migration of RRBs to Core Banking Solution System for banking operations and divergent products being offered by the Banks to its customers electronically, the internal control systems in place for ensuring safety and security of the information System were reviewed by NABARD.

'The working group on Information systems security for the Banking and Financial sector', constituted by the Reserve Bank of India stated that each bank in the country should conduct information systems audit conforming to the 'Information systems audit policy' of the bank. Further, NABARD vide their letter no /Ref No. NB.DoS.HO.POL/3634/J-1/2014-15 (Circular No 33/DoS-01/2015 dated 25.02.2015 & circular Ref. No. NB. DoS. HO. Pol. / 2116 / J-1 / 2022-23 [EC No. 193 / DoS-22 / 2022] dated 23 August 2022 asked to frame IS Audit Policy Accordingly Information Technology Department and Audit and Inspection Department of Bank has prepared the bank's Information systems audit policy'. The fundamental principle is that risk and controls are continuously evaluated by the Bank, where necessary, with the assistance of IS Audit function.

The business operations in the banking and financial sector have been increasingly dependent on the computerized information systems over the years. It has now become impossible to separate information technology from the business of the banks. Here is a need for focused attention on the issues of the governance of the information systems in computerized environment and the security controls to safeguard information and information systems. The developments in information technology have a tremendous impact on auditing. Information Technology has facilitated re-engineering of the traditional business processes to ensure efficient operations and improved communication within the organization and between the organizations and its customers. Auditing in a computerized and networked environment is still at its nascent stage in India and practices and procedures are evolving. Well planned and structured audit is essential for risk management and monitoring and control of Information Systems in any organization.

The General Manager is the owner of the IS Audit policy and any exceptions to the policy have to be approved by him.

Audit Objectives

The major purpose of audit is to ensure that the

(I) Information System on which the bank heavily depends is available for the business at all times when required,
(II) The systems are well protected against all type of losses and disasters,
(III) The information system are disclosed only to those who are authorized to see and use it and not to anyone else,
(IV) The information provided by the system is always accurate, reliable and timely.
(V) Adequate measures have been taken by the management to ensure that no unauthorized modification can be made to the data or the software in the system. As such, the IS Audit envisages physical and environmental review, system administration review, application software review, network security review, business continuity review, data integrity review etc.

Information System Audit is a series of tests that must be conducted periodically or for special purpose to ensure that adequate controls are in place over the Information System. Information System Audit is not a Financial Statement Audit and it does not test financial statement data for determining existence, completeness, rights and obligations, valuation or allocation and presentation and Disclosure.

Further, IS Audit is a systematic and independent examination of information systems environment to ascertain whether the objectives, set out to be achieved, have been met or not. Auditing is also described as a continuous search for compliance. The auditors may not necessarily examine the entire system. They may examine a part or several parts. The objectives of IS audit are to identify risks that an organization is exposed to in the computerized environment. IS audit evaluates the adequacy of the security controls and informs the Management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise in our bank. Information systems audit is an ongoing process of evaluating controls, suggest security measures for the purpose of safeguarding assets/resources, maintaining data integrity, improve system effectiveness and system efficiency for the purpose of attaining organization goals. Well planned and structured audit is essential for risk management and monitoring and control of information systems in any organization.

2.1. Safeguarding IS assets

The information systems assets of the organization must be protected by a system of internal controls. It includes protection of hardware, software, facilities, people, data, technology, system documentation and supplies. This is because hardware can be damaged maliciously, software and data files may be stolen, deleted or altered and supplies of negotiable forms can be used for unauthorized purposes. The IS auditor will require to review the physical security over the facilities, the security over the systems software and the adequacy of the internal controls. The IT facilities must be protected against all hazards. The hazards can be accidental or intentional.

2.2. Maintenance of data integrity

Data integrity includes the safeguarding of the information against unauthorized addition, deletion, modification or alteration. The desired features of the data are described hereunder:

a) **Accuracy:** Data should be accurate. Inaccurate data may lead to wrong decisions and thereby hindering the business development process.
b) **Confidentiality:** Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so. It also includes protecting the individual pieces of information that may seem harmless by the owner, but can be used to infer other confidential information.
c) **Completeness:** Data should be complete. Incomplete data loses its significance and importance.
d) **Up-to-date:** Data should be updated regularly. If the information is not up-to-date, it presents an inaccurate picture of the organization.
e) **Reliability:** Data should be reliable because all business decisions are taken on the basis of the current database.
f) **Availability:** Data should be available when an authorized user needs it. It should also be ensured that the information services are unavailable to the unauthorized users.

2.3. Maintenance of System effectiveness

An effective information system significantly contributes to the achievement of the goals of an organization. Therefore, one of the objectives of IS audit is to verify system effectiveness. It provides input to decide when, what and how the system should be improved, so that its utility to the management is maximized.

2.4. Ensuring System Efficiency

The resources used by the Information Systems such as the machines, computer peripherals, software etc. are scarce and costly. Efficient Information Systems use minimum resources to achieve the desired objectives. The ratio of the output to the input is known as efficiency. If output is more with the same or less actual input, system efficiency is achieved; or else the system is inefficient. If computerization results in the degradation of efficiency, the effort for making the process automated stands defeated. Hence, the assessment of the capabilities of the hardware and software against the workload of the environment is very essential. The IS auditors are responsible to examine how efficient the application software is in relation to the users and workload of the environment.

3. Audit Charter

The responsibility, authority and accountability of the information systems audit function is required to be appropriately documented in an audit charter or engagement letter. The IS auditor will have to determine how to achieve the implementation of the applicable IS audit standards, use professional judgment in their application and be prepared to justify departures there- from, if any. The Audit charter or engagement letter should be agreed and approved at an appropriate level within the organization. IS audit follows a three phase process, the first phase is the audit planning phase, followed by the test of control phase and finally, the substantive testing phase.

3.1. Scope of the Audit

The IS audit should cover all the computerized departments/offices/branches of the bank. Audit scope may be defined according to the audit requirement and in consultation with the user department. The usual scope that will cover:

- Determining effectiveness of planning and oversight of IT activities
- Evaluating adequacy of operating processes and internal controls
- Determining adequacy of enterprise-wide compliance efforts, related to IT policies and internal control procedures
- Cyber Security Review
- Vendor Risk Management Review
- Audit of Compliance of Regulatory Guidelines
- Backup and Recovery Controls
- Network Audit
- Compliance to the policy
- Data Localization
- API Review
- Message level Encryption
- Any other additional scope as assessed during the audit walk-through
- Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions . Further scope will also include:-

    - Implementation of IT security policy & ISMS procedures
    - Hardware / Middleware/ Interface control Review
    - General and environmental control Review
    - Access control Review (Physical & Logical)
    - Operations control Review
    - Network control Review
    - Database control Review
    - Communication control Review
    - Disaster recovery control Review
    - Conversion audit & implementation Review
    - Review of IT processes
    - Review of Performance monitoring, Scalability, availability
    - Application Control Review
    - IT Governance.

The scope of IS Audit covers all Information Systems used by the Bank in related activities viz. system planning, organization, acquisition, implementation, delivery and support to end-users. The scope also covers monitoring of implementation in terms of its process effectiveness, input/ output controls and accomplishment of system goals. The IS Audit includes the relevant processes for

planning and organizing the information systems activity and the processes for monitoring that activity. The scope of the audit will also include the adequacy and effectiveness of internal control system(s) for the use and protection of the information and the Information Systems, as under:

a)	Data	in terms of its representativeness of business and its integrity.
b)	Application systems	in terms of its functionality, controls and change management
c)	Technology	in terms of the standardization, risks, investments and returns.
d)	Hardware/ Facilities	in terms of infrastructure, maintenance and security.
e)	People	in terms of establishing segregation of duties and organizational structure, adequacy and competence.
f)	Process	In terms of Compliance to various policies with individual steps and activities.

3.2. Contents of Audit Charter

The audit charter should clearly address the three aspects of responsibility, authority and accountability of the IS auditor.

3.2.1. Responsibility should cover the following:

- Mission statement
- Aims/goals
- Scope
- Objectives
- Independence
- Relationship with external audit
- Auditee's requirements
- Critical Success Factor
- Key performance indicators
- Other measures of performance
- Providing Assurance on control Environment
- Reviewing Controls on Confidentiality, Integrity and Availability of Data Or System

3.2.2. Authority should cover the following:

- Risk assessment
- Mandate to perform IS Audit
- Allocation of resources
- Right of access to information, personnel, locations and systems relevant to the performance of the audit.
- Limitations of Scope
- Auditee's expectations
- Organizational structure, including reporting lines to the Board of Directors/Higher Management/Designated authority.
- Gradation of IS Audit officials/staff

3.2.3. Accountability should cover the following:

- Reporting lines to Senior management/ Board of Directors/ Designated Authority through proper channel
- Assignment performance appraisals
- Personnel performance appraisals

- Staffing/ career development
- Auditee's right
- Independent Quality reviews.
- Assessment of compliance with standards.
- Benchmarking performance and functions.
- Assessment of completion of the audit plan.
- Comparison of budget to the actual costs.
- Agreed actions e.g. penalties when either party fails to carry out his responsibilities.
- Co-ordinate with and provide Oversight over other control functions like risk management, security and compliance
- The policy should also cover Audit Rating Methodology and Quality Assurance Reviews. There could also be annual review of IS Audit Policy or Charter to ensure continued relevance.

3.3. Communication with the Auditee

The audit charter forms a sound basis for communication with the auditee and should include consideration of the following:

- Describing the service, its scope, its availability and timeliness of delivery.
- Providing cost estimates or budgets, if they are available.
- Describing problems and possible resolution of them.
- Providing adequate and readily accessible facilities for effective communication.
- Determining the relationship between the service offered and the needs of the auditee.

  The Audit Charter forms a basis for communication with an auditee. It should include relevant references to service-level agreements for aspects like the following, as applicable:
  - Availability for Unplanned Work
  - Delivery of reports
  - Costs
  - Response to Auditee's Complaints
  - Quality of Service
  - Review of Performance
  - Communication with the Auditee
  - Needs Assessment
  - Control Risk Self-assessment
  - Agreement of Terms of Reference for Audit
  - Reporting Process
  - Agreement of Findings

3.4. Quality Assurance process

The IS auditor should consider establishing a quality assurance process (e.g. interviews, customer satisfaction surveys, assignment performance surveys etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

3.5. Engagement Letter

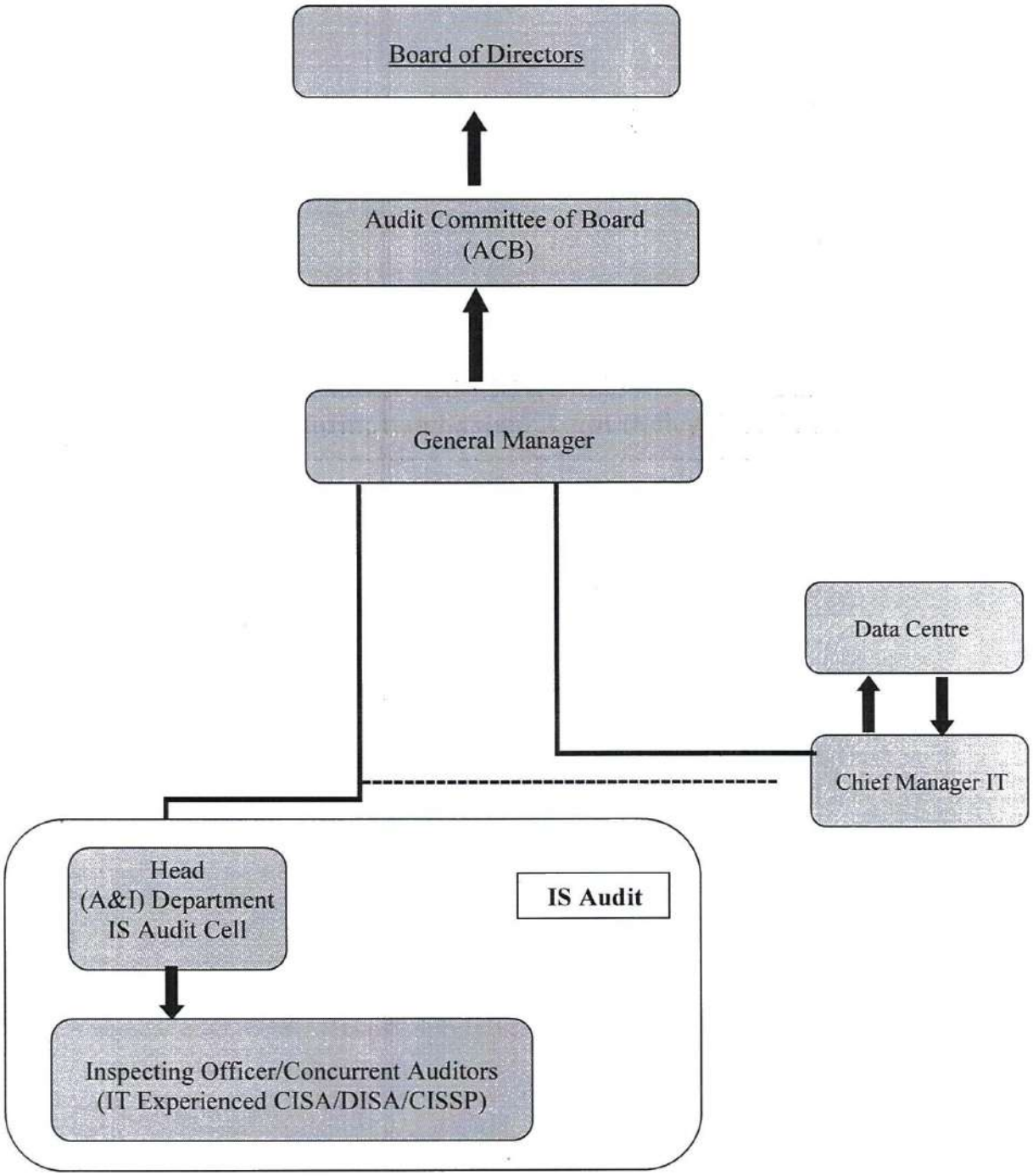
Engagement letters are often used for individual assignments, setting out the scope and objectives of a relationship between the external IS audit agency and Bank. The engagement letter should clearly address the three aspects of responsibility, authority and accountability.

3.6. Responsibilities of IS Audit

The involvement of IS auditor for a system starts from the initial stage of a newly developed or acquired package. The auditor should be involved during all the stages of systems development life cycle (SDLC) process. Implementation of any additional control measures will be easier and cost effective if detected at the development stage. The IS auditors should be well prepared, as under, to perform IS auditing:

1) Understand, recognize and report potential and actual risk.
2) Comply with the IS security policy and procedures and guidelines issued by the bank.
3) Reporting incidents to the Coordination committee without delay.
4) Immediately clarifying areas of doubt concerning security, audit or interpretation of this policy.
5) Making recommendations for improving controls.
6) A general understanding of the operating systems in use.
7) Thorough knowledge of application software in use.
8) Knowledge of automated operations, methods of storing and retrieval of data and controls used in the systems.
9) Knowledge of the methodology used in data processing.
10) IS auditors for auditing complex systems requires substantial knowledge about development, implementation and operation of the systems. A thorough understanding of various controls in the development of systems, maintenance of data and network management is essential.
11) An understanding of the emerging technologies, capacity to determine their impact on controls, ability to change audit procedures suitably and to develop evidence collection tools and techniques.
12) IS auditors, to be engaged, should maintain technical proficiency and keep themselves abreast of the current changes in the procedures, technologies adopted and the functions computerized by the bank.
13) Ability to identify general security measures including risk analysis.
14) Capabilities to render constructive disaster assessment.
15) Sound knowledge of the organization's accounting practice and record keeping requirements.
16) Ability to investigate thoroughly and to document the investigation work.
17) The audit process requires initiative, thoroughness and tact while addressing an audit assignment.
18) IS audit call for understanding and the capabilities to analyze and offer constructive comments on the Information Systems Security and Controls.
19) All material irregularities are required to be reported and IS auditor should report all the important findings.
20) The IS auditor should be aware of the situation where too much trust has been placed on one individual. One person acting alone could commit an error willfully or unknowingly in the bank. This is important in those transactions which are perceived to be of high risk.
21) Capacity to plan and supervise IS audit to assure that the audit meets the desired objectives, as set out in the audit assignment, efficiently.
22) Knowledge of the basics in computer programming would help in having clarity of approach.
23) IS Auditor should exercise due professional care, including observance of applicable professional auditing standard.

3.7. Organization & Reporting of the IS Audit



3.7.1 Organization Structure

The **Information System audit cell** shall be headed by a senior officer, not below the rank of an Assistant General Manager /Chief Manager (CISA/DISA qualification will be preferred) be who has a thorough knowledge in Banking Operations and Information Technology.

3.7.2 Reporting Lines

The AGM/Chief Managers looking after IS Audit will report to the General Manager. The AGM/Chief Manager (Internal Audit,) is the head of the Audit & Inspection Department which functions independently. The AGM/Chief Manger (Internal Audit,) is the convener of the Audit Committee of the Board –ACB.

3.7.3 Roles & Responsibility

3.7.3.1 Audit Committee of the Board

- The ACB, should provide an effective oversight of the IS Audit function and devote appropriate time to the IS audit findings identified during IS Audits.
- The ACB should approve the annual IS audit plan of the Bank.
- The ACB should review Senior Management decision on all significant/ critical /high risk observations and recommendations presented by the IS Audit Cell through the A &I and I.T department.
- Review matters reported by the IS Audit Cell through the A &I and I.T department on issues where the residual risk accepted by the user department / Senior Management is high.

3.7.3.2 Internal Inspection & Audit Department of Head Office

- Review compliance status of the directions given by ACB and other authorities in the area of IS audit
- Reviewing the scope and nature of work of the Internal Audit Department and annual review of audit related polices for putting up to ACB.
- Review and recommend Annual Risk Based Audit Plan to ACB for consideration and approval
- To review all critical observations / significant audit findings and their compliance before putting up to the ACB.
- To give directions to the IS Audit cell in carrying out the IS Audit activities in an effective and efficient manner.
- To review the delays in timelines in closure of the critical observations.
- To review IS Audit policy level changes and approve the IS audit manual.
- Give the overall guidance and direction in preparation of the Annual audit Plan of the IS Audit Cell in alignment with the annual audit plan of the Bank.
- Place before the ACB the annual IS audit plan for approval,
- Place before the ACB the significant /critical /high risk findings of various IS Audits.
- Monitor to ensure that the critical IS audit observations are closed in a timely manner.

3.7.3.3 Chief IS Auditor

- Overall direction and guidance to the IS Audit activity of the Bank in compliance with the IS audit policy & Manual of the Bank and applicable regulations.
- Preparation of annual audit plan following a Risk based approach.
- Coordination and completion of the Planned audit activity.
- Allocate audits following a rotation system ensuring that the same auditor will not audit the same application / infrastructure audited in the preceding year, depending upon available resources.
- Follow up on audit findings /compliance and reporting on significant audit findings to ACB

- Place before ACB on delays beyond the timelines in closure of the critical observations, matters on acceptance of high residual risk by the user department / senior management.
- Assistance in timely review of the IS Audit policy.
- Coordination with CISO for policy level changes.
- Procurement / development of IS Audit tools.

3.7.3.4 Head (Information System Audit)

- IS Audit of new and existing applications – IT Architecture, Development of software, Operations System controls, Application Systems and controls, Database Controls, Network Management Audit
- IT Governance related issues
- Review of application controls, configuration review etc.
- Coordinates audits carried out by external auditors.

3.7.3.5 Head (IS Compliance Audit)

- Bank's compliance with legal and regulatory requirements (RBI circulars & guidelines in respect of IS audit related area only)
- Audit of Business Continuity Management.
- Audit of implementation of IT/ IT security policy /guidelines /procedures of the Bank.
- Monitor IS audit activities carried by Inspecting officers/concurrent auditors.
- Coordinate the activities of the concurrent audit and monitoring team of CBS operations constituted as per authority.
- Provide necessary support on strengthening of control mechanism carried by HO/ROs.
- Coordinate training to Concurrent Auditors/Internal Inspecting Officers and updating Audit program sheets used by inspecting officers.

3.7.3.6 IS Auditor

Conduct the assigned IS audits and submit report in compliance with the IS audit policy of the Bank and other regulatory guidelines within allotted man- days. IS auditors of all levels have to conduct the assigned audits and submit reports duly adhering to the responsibilities as mentioned in 3.6

The inspecting officers attached to A & I department & concurrent auditors should conduct the IS audit of Branches / Administrative offices etc. under the guidance of A &I department at HO and in compliance with the IS audit Policy.

4. Types of Risks

The deployment of Information Technology, both in the front and back office operations and the subsequent Core Banking Solution has facilitated greater systemic efficiency in our bank. It has at the same time, introduced new areas of risk. Risk is inherent in banking and financial activities. However, risk in a computerized and networked environment is multifarious such as operational risk, reputational risk, credit risk, liquidity risk, interest rate risk etc.

4.1. Information Systems audit

Information systems audit for Banks should be conducted in three phases. The first phase is the planning phase whereby an IS auditor must identify the various risks and exposures and the security controls, which provide safeguards against these exposures. In the second phase, the security controls are tested. The third phase is the substantive testing phase, where individual transactions are tested may be by using computer assisted audit tools and techniques. There are five basic approaches for testing the application controls using CAATT (Computer Assisted Audit Tools & Technology).

- Test data Method
- Base case system evaluation
- Tracing

- Integrated Test facility
- Parallel Simulation

5. Information Systems Audit Approaches

There are three audit approaches for conducting Information systems audit viz. Audit around the computer, audit through the computer and audit with the computer.

5.1. Auditing around the computer

Under this approach, the emphasis is on checking the correctness of the output data/ documents with reference to the input of a process without going into details of the processing involved.

The approach may be used when an application system uses a generalized package that is well tested and used by many users as its software platform. Auditing around the computer is a simple approach. It does not provide any information about the system's ability to cope with the changes. This method cannot be used for complex systems.

5.2. Auditing through the computer

Auditing through the computer requires fair knowledge of technology, Software, hardware and system development methodology. Under this approach, the computer programs and the data constitute the target of IS audit. Compliance and substantive tests are performed on the computer system, its application and data. This approach increases the IS auditor's confidence in the reliability and applicability of the evidence/ information collected and evaluated.

5.3. Auditing with the computer

Under this approach, the computer system and its programs are used as tools in the audit process. The objective is to perform substantive tests using the computers and its programs. The data from the auditee's computer system are retrieved to an independent environment.

The following Tools and Techniques may be used during the process of IS Audit.

5.4. Computer Assisted Audit Tools (CAATs)

CAATS are efficient and effective ways to audit system generated files, records and documents and to evaluate internal controls in any application systems. They are the practical means for conducting audit, wherever the information is available on magnetic media. Various audit software may also be used for the same purpose.

5.4.1. Test Data Techniques

A representative sample of data transactions is entered into the auditee's computer system and the results are compared with the predetermined results. CAATs are used to test the details of the sample transactions, the balances of the accounts, to identify usual fluctuations, if any and general controls like accessing the program libraries.

5.4.2. Generalized Audit Software (GAS)

It is the most widely used techniques in conducting IS audit. Its use is limited by the skills of the personnel conducting the audit. ACL, IDEA are the two most important GAS available at present. It is really a data analysis tool. It has the capabilities for compliance and substantive testing.

6. Audit Methodology

The IS audit work includes manual procedures, computer assisted procedures and fully automated procedures, depending on whether it is around through, with or a combination of all these types of audit. In many cases, a combination of these techniques is required.

6.1. Coordination Committee for IS Audit

IS Audit Coordination Committee is to be formed for the purpose of Critical system / application IS Audit / IT infrastructure audit of DC/DR etc. The coordination committee will decide on the scope of the audit, facilitating the conduct of the IS audit during the planning and execution stages, facilitating provision of all the required documents /guidelines /operational manuals, facilitating test environment / interaction with the user and developers, follow up with the issues raised during the course of audit and monitor the audit process from time to time. This committee will bring the IS Audit process of a system into a logical conclusion and take measures to implement all the accepted modifications suggested by the IS Auditor. IS Coordination committee will consist of the representatives from A &I and I T department, user department, Development team. In respect of audit of smaller applications the business owner / application owner will nominate a single point of contact Data Centre to facilitate the audit, which will carry out the above role.

6.2. Coverage of IS Audit

An Audit Universe is an outcome of the risk assessment process. It will define audit areas to be covered. It will include all areas related to IT including resources, processes, applications, data, technology, networking, data center etc.

The audit frequency will be based on the criticality and the business impact of the application and in an audit cycle of 3 years all the applications will be covered. The periodicity and coverage will be guided by the following table

Sr.	Name of the application / Type of the system	By	Frequency
1	Critical Systems with high business impact	IS Auditor – DISA/CISA/CISSP qualified Internal / external	Yearly
2	Other Critical Systems/Medium Risk	IS Auditor – DISA/CISA/CISSP qualified Internal / external	Once in 18 Months
3	Non Critical Systems/Low Risk	IS Auditor – DISA/CISA/CISSP qualified Internal / external	Once in 3 years.
4	Branches	IS Auditor – Internal or external	Yearly

Note: Suggested check list for the guidance of Auditor carrying out IS Audit is annexed with the policy.

6.3. Audit activity

The audit activity is broadly divided into 5 major steps for the convenience and effective conduct of audit.

- Planning IS Audit
- Tests of controls
- Tests of transactions
- Tests of balances
- Completion of audit
- Compliance Review

6.4. Planning IS Audit

The IS auditor is to plan the IS audit coverage to address the audit objectives and to comply with applicable law and professional auditing standards. This plan is to be discussed with the user and development team before finalizing the audit program. When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet the audit objectives, and its varying levels of reliability. Among the things to be considered are the independence and qualification of the provider of the audit evidence. Physical audit evidence is generally more reliable than the representations of an individual.

The IS Auditor should develop and document a risk-based audit approach. He should develop and document an audit plan detailing the nature and objectives, timing and extent, and resources required. He should develop an audit program and procedures. The entire Audit program sheet should be approved by the Audit Committee of the Board.

As a part of the planning process, IS auditors should obtain an understanding of the auditee department/office/organization and its processes. It includes understanding of the objectives to be accomplished in the audit, collecting background information, assigning appropriate staff keeping in mind skills, aptitude etc. and identifying the areas of risk. Risk analysis of the operational system is carried out to identify the system with highest risks, considering the critical nature of the information processed through such system as well as the number and the value of the transactions processed. This is to identify the systems having the highest risk and to decide on the extent of the detailed analysis and testing to be conducted on those systems. This will form the basis of Risk based Internal Audit (RBIA).

An effective IS Audit program addresses IT risk exposures throughout a bank, including areas of IT management and strategic planning, data centre operations, client or server architecture, local and wide-area networks, telecommunications, physical and information security, electronic banking, applications used in banking operations, systems development, and business continuity planning. A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT related risks of every size and complexity. Effective programs are risk-focused, promote sound IT controls, ensure timely resolution of audit deficiencies, and inform the Audit Committee of the effectiveness of Risk Management practices and internal control systems. In the past, the Internal Audit concentrated on transaction testing, testing of accuracy and reliability of accounting records and financial reports, integrity, reliability and timeliness of control reports, and adherence to legal and regulatory requirements. However, in the changing scenario, there is an increased need for widening, as well as redirecting, the scope of Internal Audit to evaluate the adequacy of IT Risk Management procedures and internal control systems. To achieve these, banks are moving towards risk based internal audit, which include, in addition to selective transaction testing, an evaluation of the Risk Management systems and control procedures prevailing in a bank's operations Risk-based Internal Audit (RBIA) approach helps in planning the IS Audit.

It includes the following components:

- Understanding IT Risk Assessment Concepts
- Adopting a suitable IT Risk Assessment Methodology-used to examine auditable units in the IS audit universe and select areas for review to include in the IS Annual Plan that have the greatest risk exposure
- Steps involved are:
  - Step 1: System Characterization
  - Step 2: Threat Identification
  - Step 3: Vulnerability Identification
  - Step 4: Control Analysis
  - Step 5: Likelihood Determination
  - Step 6: Impact Analysis
  - Step 7: Risk Determination
- As a part of RBIA, planning the IS Audit involves the following:

Defining the IS Audit Universe

This covers the IS Audit Universe, which defines the areas to be covered

Scope for IS Audit

This addresses the scope requirements and includes:

- Defining control objectives and activities
- Considering materiality
- Building a fraud risk perspective

Planning Execution of an Audit

This describes the steps of a planning process before IS Audit starts execution of the plan

- Documenting an audit plan
- Nature and extent of test of control
- Sampling techniques
- Standards and frameworks
- Resource management

The above components are clarified in the sub-sections below:

Risk Based IS Audit

This internal audit approach is aimed at developing a risk-based audit plan keeping in mind the inherent risks of a business or location and effectiveness of control systems managing inherent risks. In this approach, every bank business or location, including risk management function, undergoes a risk assessment by the internal audit function. RBI issued the "Guidance Note on Risk-based Internal Audit" in 2002 to all scheduled commercial banks, introducing the system of "Risk-based internal audit". The guidance note at a broad-level provided the following aspects:

- Development of a well-defined policy for risk-based internal audit
- Adoption of a risk assessment methodology for formulating risk based audit plan
- Development of risk profile and drawing up of risk matrix taking inherent business risk and effectiveness of the control system for monitoring the risk
- Preparation of annual audit plan, covering risks and prioritization, based on level and direction of each risk
- Setting up of communication channels between audit staff and management, for reporting issues that pose a threat to a bank's business
- Periodic evaluation of the risk assessment methodology
- Identification of appropriate personnel to undertake risk-based audit, and imparting them with relevant training
- Addressing transitional and change management issues

The overall plan, arrived at, using the risk assessment approach enables the Internal Audit to identify and examine key business areas that have highest exposure and enables effective allocation of Audit resources. As stated earlier, IS Audit, being an integral part of the Internal Audit, there is a need for IS Auditors to focus on the IT risks, related to the high-risk business areas identified by the Internal Audit for review during a year. This enables the IS Audit to provide an assurance to the management on the effectiveness of risk management and internal controls underlying the high-risk business processes, which when read in conjunction with the Internal Audit reports, provides a holistic view of the effectiveness. Risk-based IS Audit needs to consider the following:

- Identification of an institution's data, application, technology, facilities, and personnel
- Identification of business activities and processes within each of those categories
- Profiles of significant business units, departments and product lines and systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution
- Use a measurement or scoring system that ranks and evaluates business and control risks for business units, departments and products
- Includes Board or Audit Committee approval of risk assessments and annual Risk-based Audit Plans that establish audit schedules, cycles, work program scope and resource allocation for each area audited
- Implementation of the Audit Plan

Adopting a Suitable Risk Assessment Methodology

The IS Auditor must define, adopt and follow a suitable risk assessment methodology. This should be in consonance with the focus on risks, to be addressed as a part of the overall Internal Audit Strategy.

6.5. Tests of controls:

During this phase of IS audit, internal controls are tested to evaluate whether they operate effectively. This includes testing of management controls and application controls. The objective is to evaluate the reliability of the controls and find out weaknesses of the controls for meeting the IS audit objectives. IS auditor is required to make recommendations to rectify the weaknesses, observed during the course of an IS audit. During this phase, IS auditor will satisfy themselves regarding the following:

- Identification
- Implementation
- Existence
- Adequacy
- Documentation
- Maintenance
- Monitoring of controls

6.6. Tests of Transactions

Tests of transactions are used to evaluate whether erroneous transactions have led to a material misstatement of the financial information and whether the transactions have been handled effectively and efficiently. The objective is to evaluate data integrity. Some of such tests include the tracing of journal entries to their source documents, the testing of computational accuracy, the study of the transaction logs etc.

6.7. Tests of Balances

During this phase of IS audit, final judgment is made on the extent of the losses or account misstatement that occur when information systems fail to safeguard assets, maintain data integrity and achieve system effectiveness and efficiency goals. As regards the safeguarding of assets and data integrity, objectives, the typical substantive tests used are confirmation of the receivables, physical verification of inventory and recalculation of depreciation of fixed assets. Regarding the system effectiveness and system efficiency objectives, the tests to be conducted are in the process of evolution. For example, the shortcomings in the Information Systems planning may have resulted in the purchase of inappropriate hardware. The system may provide outputs, but not of the required standards to make high quality decisions. During this phase Generalized Audit Software is used.

6.8. Completion of Audit

This is the final stage of IS Audit. Auditors are required to form their opinion, clearly indicating their findings, analysis and recommendations. Potential IS Audit findings should be discussed with the appropriate/ authorized personnel throughout the course of IS auditing. Preliminary conclusions and the audit findings should be presented to the auditee during an exit conference. All potential findings with sufficient merits and preliminary IS Audit recommendations should be included for discussion in the exit conference. The exit meeting should document and include the auditee's comments and questions concerning the preliminary IS audit recommendations. The draft audit report should be the natural extension of the exit conference materials along with the discussions that took place during the exit meeting. Once the auditee's response has been received, the final audit report should be prepared and submitted to the designated authority (GM Internal Audit).

Work papers used in the auditing should be well organized, clearly written and address all the areas included in IS audit. IS audit work papers should contain sufficient evidence/ information of the tasks performed and the conclusions reached, including the result achieved, issues identified and authorized signature approving the final opinion.

6.9. Sub-system Factoring

IS Audit is generally an exercise dealing with the complex Information Systems. In order to understand the complex system, it is always advisable to break the system into sub-systems. A sub-system is a component of a system that performs some basic

functions needed by the overall system to attain its basic objectives. This process is called factoring. The process of factoring terminates when it is felt that the system has been broken into the sub-systems, small enough to be understood and evaluated.

6.10. Broad Framework for conducting IS Audit

A broad framework can be formed from the basic objectives of IS Audit. In addition to this, IS audit evaluates the organizational setup and quality of administration. It should be noted that IS audit is not limited by laid down procedures. It is also important to keep's one's eyes and ears open. The IS auditors should therefore, analyze what they observe and hear.

The major concerns are:

A. Safeguarding Assets

- Environmental controls
- UPS
- Electrical Lines
- Data cabling
- Fire & Gas protection
- Insurance
- Annual Maintenance Contract
- Logical access controls (Operating & Application System)

B. Data Integrity

- Data Input controls
- Data processing Controls
- Patch program
- Purging & Retention of data files.
- Data backup
- Restoration of data

C. Business Continuity Planning

- Documented DRP
- Output reports
- Version Control
- Antivirus software

D. System Effectiveness & Efficiency

E. Organization & Administration.

6.11. Audit process

During the course of the audit, the information systems auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis, on-line tests and interpretation of evidence. The IS auditor should design and select an audit sample and evaluate the sample results. Appropriate sampling and evaluation will meet the requirements of 'sufficient, reliable, relevant and useful evidence' and 'supported by appropriate analysis'. The IS auditor should select the techniques, which result in a representative sample statistically for performing the compliance or substantive testing. The IS Auditor may use acceptable Computer assisted audit techniques (CAAT) for the purpose of data evaluation, extraction or analysis. He may use test data into a live system in association with the user department and remove all such test data before completion of audit process.

6.12. Audit Evidence

The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results and he should evaluate the sufficiency of audit evidence obtained during the audit. In general terms, the reliability of audit evidence is greater when it is in written form, rather than oral expressions, obtained from independent sources and obtained by the IS auditor rather than from the entity being audited.

In respect of audit evidence / information processed by Electronic Data Interchange (EDI), Document Image Processing (DIP) and dynamic systems such as spreadsheets etc. may not be retrievable after a specified period of time, if changes to the files are not controlled or the files are not backed up. Since it is not possible for the IS auditor to make multiple copies of system documents, IS auditor would sign various documents produced for the purpose of audit and would advise auditees to preserve these documents for further reference.

Audit evidence should be secured against unauthorized access and modification. All audit evidences should be retained for at least seven years as per the applicable law in India. In those situations where the IS auditor believes sufficient audit evidence cannot be obtained, the IS auditor should disclose this fact in a manner consistent with the communication of the audit results.

6.13. IT Governance

The IS Auditor should review and assess whether the IS function aligns with the organization's mission, vision, values, objectives and strategies. He should review whether the IS function has a clear statement about the performance expected by the business and assess its achievement.

The IS Auditor should review and assess the effectiveness of IS resources and performance management. They should review and assess compliance with legal, environmental and information quality, and fiduciary and security requirements. A risk based approach should be used by the IS auditor to evaluate the IS function. He should also assess the risks that may adversely affect the IS environment.

7. Risk assessment in Audit Planning

The IS auditor should use an appropriate risk assessment technique or approach in developing the overall IS audit plan and in determining priorities for the effective allocation of IS audit resources. When planning individual reviews, the IS auditor should identify and assess risks relevant to the area under review.

Risk assessment is a technique used to examine auditable units in the IS audit universe and select areas for review to include in the IS annual plan that have the greatest risk exposure. Risk assessment exercises to facilitate the development of the IS audit plan should be carried out and documented at least on an annual basis. Organizational strategic plan, objectives and the enterprise risk management framework should be considered as part of the risk management exercise.

The use of risk assessment in the selection of audit projects allows the IS auditor to quantify and justify the amount of IS audit resources needed to complete the IS audit plan or a particular review. Also, the IS auditor can prioritize scheduled reviews based on perceptions of risk and contribute towards the documentation of risk management frameworks.

An IS auditor should carry out a preliminary assessment of the risk relevant to the area under review. IS audit engagement objectives for each specific review should reflect the results of such a risk assessment. Following the completion of review, the IS auditor should ensure that the organization's enterprise risk management framework or risk register is updated to reflect findings and recommendations of the review and subsequent activity.

7.1. Risk Based IS Audit approach

Risk-based Internal Audit (RBIA) approach helps in planning the IS Audit. RBI Guidelines viz Gopalkrishna Committee Recommendations includes an Understanding of IT Risk Assessment Concepts & adopting a suitable IT Risk Assessment Methodology to examine auditable units in the IS audit universe. The focus will be on areas that have the greatest risk exposure, which determines the frequency of the audit. Risk based auditing require a four step process.

- Define the processes covering an Organization's operations.
- Rank and score processes on the basis of their relative risks.

- Assess process risks with an emphasis on higher-risk areas
- Initiate actions to install controls over higher-risk processes.

IS Audit should provide an assurance to the management on the effectiveness of risk management and internal controls underlying the high-risk business processes. Risk-based IS Audit needs to consider the following:

- Identification of an institution's data, application, technology, facilities, and personnel
- Identification of business activities and processes within each of those categories
- Profiles of significant business units / departments , and their associated business risks and control features
- Use a measurement or scoring system that ranks and evaluates business and control risks for business units / departments
- Preparation of the annual Risk-based Audit Plans based on the risk assessment.
- Implementation of the Audit Plan

The IS audit universe will be identified covering all the applications in use in the Bank. All the applications criticality will be measured on the basis of Confidentiality, integrity, availability, reputation, and legal risks with risk ranking as high, medium, and low against each risk.

The business impact will be based on classification of an IT system as Critical System with Operational risk prone area, Critical System with high business impact area, other critical systems, and non-critical systems.

The audit frequency will arrive on the basis of a composite factor. The composite factor will be on multiplication of the risk factor based on the criticality of the application with the business impact of the system / application.

8. Audit materiality and Audit Risk

The IS Auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures. The IS Auditor should consider the cumulative effect of minor control deficiencies or weaknesses and absence of controls to translate into significant deficiency or material weakness in the Information systems. The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness.

Audit risk is the risk of the IS Auditor reaching an incorrect conclusion based upon audit findings. The IS Auditor should also be aware of the three components of audit risk, namely, inherent risk, control risk and detection risk. While planning and performing the audit, the IS Auditor should attempt to reduce audit risk to an acceptably low level and meet the audit objectives. This is achieved by appropriate assessment of IS and related controls.

Weakness in control is considered 'material' if the absence of the control results in failure to provide reasonable assurance that the control objective will be met. A weakness classified as material implies that controls are not in place and/or controls are not in use and/or controls are inadequate. A material weakness is a significant deficiency or a combination of significant deficiencies that results in more than a remote likelihood of an undesired events not being prevented or detected.

There is an inverse relationship between materiality and level of audit risk acceptable to the IS auditor, i.e. the higher the materiality level, the lower the acceptability of audit risk, and vice versa. This enables the IS Auditor to determine the nature, timing and extent of audit procedures. For instance, when planning for a specific audit procedure, the IS auditor determines the materiality is lower, thereby increasing the audit risk. The IS auditor would then want to compensate by either extending the test of controls (reduce assessment of control risk) or extending the substantive testing procedures (reduce assessment of detection risk). In determining whether a control deficiency is a significant deficiency or a material weakness, the IS auditor should evaluate the effect of compensating controls and whether such compensating controls are effective.

8.1. IT Risk assessment methodology for IS Audit

The IS auditor is concerned with high risk areas and weak controls. During the audits, the IS auditor should identify critical control systems that address high inherent risks and ensure that the controls are effective. He has to identify the areas where the residual risk is at an unacceptably higher level.

The IS auditor will carry out risk assessment to understand the Criticality of the risks and the controls that are placed to mitigate them. The risk template will be prepared meeting the specific audit requirements.

The following factors will be considered by the IS Auditor during the risk assessment process / preparation of the template.

* The criticality of the activity
* The fall back arrangements placed to continue the activity, if the system has problems.
* The sensitivity of the function to the executive management
* Materiality of the activity with regard to its effect on the functioning of the organization.
* The complexity of the system – risk factors or potential for errors or misappropriation to go undetected because of the complexity of the system.

The following IS application risks will also be considered

* Inaccuracy of processing
* Incompleteness of processing
* Non-availability
* Logical access controls.

From the business perspective, the IS Auditor will classify an IT system as Critical system with operational risk prone area, critical system with high business impact area, other critical systems, and non-critical systems.

9. Information Technology, Security issue & IS Audit

Information Technology offers an easy and efficient way to collect, store, process and transmit information to any organization. Vital business decisions are made by the organizations on the basis of this information and therefore, it is imperative to ensure that right information is available at the right time to the right people. Further, adequate security controls have also to be in place in an organization to ensure that the information and the information systems remain inaccessible to unauthorized persons. Information stored in the computer systems and transmitted through networks will be required to be protected. The protection of information becomes critical, when it is fund-based or represents sensitive/ confidential data like personnel records.

The need for security controls assumes greater importance in view of the advent of Internet. Connecting to the internet without strong security architecture in place can have severe consequences for an organization. The extent of criminal activities in the internet based environment is growing along with advancement in Information Technology. For e-banking related product on the net we have to address the following security issues:

- Unauthorized access to Information
- Loss/Manipulation/Modification of data
- Loss of confidential information.
- Problem inherent to open network.

Our organization will be required to identify the events and circumstances, whose occurrence could result in a loss to the organization. These are called exposures. Controls are those acts/measures which the organization must implement to minimize these exposures. Controls are broadly of the following types:

- **Deterrent Controls**: Deterrent controls are designed to deter unauthorized people, internal as well as external, from accessing the information.
- **Preventive Controls**: Preventive controls prevent the cause of exposure from occurring or at least minimize the probability of the occurrence of unlawful events.
- **Detective Controls**: When a cause of exposure has occurred, detective controls report its existence in an effort to arrest further damage or minimize the extent of damage.
- **Corrective Controls**: Corrective controls are designed to help the organization recover from a loss situation. Business continuity planning is a corrective control. Without corrective controls in place, the organization will suffer from the risk of loss of business and other losses, due to its inability to recover essential IT based services, information and other resources after the disaster has taken place.

IS auditors will be required to ascertain that adequate control exists to cover each likely unlawful event. If the unlawful event is covered by a control, the IS auditor will be required to evaluate whether the control is operating effectively. If more than one control covers an unlawful event, the IS auditors will be required to verify that all these controls operate effectively.

10. Audit Considerations for Irregularities and illegal acts:

Due professional care and the observance of the internationally accepted professional auditing standards (e.g. COBIT, IS27001) have to be exercised by the IS Auditor in all aspects of IS auditing. The Information systems auditor will be required to plan the information systems audit work to address the audit objectives and to comply with internationally accepted professional auditing standards. Further, during the course of IS auditing, the Information systems Auditor will be required to obtain sufficient, reliable, relevant and useful evidence/ information to achieve the audit objectives effectively. In addition, the audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence/ information by the IS auditor.

Some irregularities may be considered fraudulent activities. The determination of the fraudulent activities depends on the legal definition of fraud. Irregularities include, but are not limited to, the deliberate circumvention of controls with the intent to conceal the perpetuation of fraud, the unauthorized use of the assets or services etc. and the abetting or helping to conceal these types of activities.

In planning and performing the audit to reduce audit risk to a low level, the IS auditor should consider the risk of irregularities and illegal acts. The IS auditor should maintain an attitude of professional skepticism during the audit, recognizing the possibility that material misstatements due to irregularities and illegal acts could exists, irrespective of his/her evaluation of the risk of irregularities and illegal acts. The IS auditor should obtain sufficient and appropriate audit evidence to determine whether management or others within the organization have knowledge of any actual, suspected or alleged irregularities and illegal acts and he should consider unusual or unexpected relationships that may indicate a risk of material misstatements due to irregularities and illegal acts. He should perform procedures to test the appropriateness of internal control and the risk of management override of controls.

If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, the IS auditor should communicate these matters in a timely manner to the In Charge of IS Audit Cell. The IS auditor should document all communications, planning, results, evaluations and conclusions relating to material irregularities and illegal acts that have been reported to management. The risk of not detecting a material misstatement resulting from an illegal act is higher than the risk of not detecting a material misstatement resulting from an irregularity or error, because illegal acts may involve complex schemes designed to conceal or hide events or intentional misrepresentations to the IS auditor.

11. Resource Personnel & Skills

Product, process and people are the three most important components of any successful operation. The requirement of various types of internal IS auditor will follow the underlying matrix in our organization. Quality of internal IS auditor will play an important role in defining as well mitigating the risk, exposure and control system in any application.

Sr.	Type of Audit	Required Personnel	Qualification
1.	IS Audit of Branches	Internal/ External	Inspecting Officer / CISA/DISA qualified external auditor
2.	IS Audit of Admin. Offices	Internal/ External	IT experienced (CISA/DISA qualified external auditor)
3.	(SW) Application Systems Audit	Internal/ External	IT experienced (CISA/DISA/CISSP qualified auditor)
4.	Conversion Audit	Internal/ External	IT experienced (CISA/DISA/CISSP qualified auditor)
5.	Data Audit	Internal/ External	IT experienced (CISA/DISA/CISSP qualified auditor)
6.	DC & DR site (IT Infra)	Internal/ External	IT experienced (CISA/DISA/CISSP qualified auditor)
7.	Highly Technical specialized installation like SITB, SWIFT, MICR, RBO,NAP etc.	Internal/External	IT experienced (CISA/DISA/CISSP qualified auditor)

11.1. Selection of IS Auditors

The IS auditor to be selected for conducting any IS audit have to be technically competent, having skills and knowledge necessary to perform the audit work. He may be an in-house staff or outsourced. The suggestions of regulator should be strictly followed in conducting IS audit. The auditor should be independent of auditee. The IS auditor should preferably be of CISA/DISA/CISSP qualified and with sufficient branch banking experience.

11.2. Independence

The IS audit function is to be sufficiently independent of the area being audited to permit objective completion of the audit assignment. The auditor should be independent of the auditee in attitude and appearance.

11.3. Continuous professional education

The IS Auditor should be professionally competent, having the skills and knowledge to conduct the audit. The Information systems auditor is to maintain professional and technical competence through appropriate continuing professional education and training. Bank should encourage officers in IS Audit department to acquire more and more professional qualification related to their area of operations. The IS auditor need to be trained on contemporary topics of IT, Audit & security at regular interval. They should be encouraged to acquire CISA, CISSP, CISM, CGEIT, CEH, CQA, Lead Auditor and related qualification in IS Audit field. All IS auditor is required to attend the annual conference of their affiliated organization for the purpose of acquainting with the latest development and keep themselves updated with technological developments.

11.4. Periodicity of Audit

The periodicity of the audit should be based on the risk assessment of the system. Usually a CBS branch should be audited from IS audit angle once in a 12/18 months by A&I Department along with regular inspection of branch. Critical Systems / applications with operational risk prone area are to be audited once in 12 months or any major modification done, whichever is earlier. VAPT for web based customer facing applications is to be carried out as per Bank's IT security policy. Conversion audit i.e. migration audit is to be done within 30 days of conversion / migration. All systems, domains and processes should be covered once with in a period of three years (Refer: RBI/2010-11/494 dated 29.04.2011).

IS Audit of applications / systems / branches may be / preferably be undertaken prior to the statutory audit so that the IS Audit reports are available to the statutory auditors well in time for examination and incorporating comments, if any, in the their audit reports. (Refer RBI/2004/191 dated 30.04.2004).

11.5 Continuous Audit

A continuous audit approach allows internal auditors to fully understand critical control points, rules, and exceptions. With automated, frequent analyses of data, they are able to perform control and risk assessments in real time or near real time. They can analyze key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk.

With continuous auditing, the analysis results are integrated into all aspects of the audit process, from the development and maintenance of the enterprise audit plan to the conduct and follow-up of specific audits. The implementation of concurrent auditing in critical areas of Data center should also be a part of Continuous Audit.

11.6 Vendor Audit

Bank may avail vendor services for various information System related activities. The vendors service delivery can be of the below modes:

- **Standalone:** Servicing from his own premises and using his own IT computing resources including network resources.
- **Bank Connected:** Servicing from his own premises but using Banks IT computing resources and connected to Banks network for data sharing.
- **Onsite:** Servicing from Banks premises using Banks IT computing resources

For each of the above scenarios, following periodic compliance report should be kept in record by the business team for review by the auditor during IS Audit. Further all other terms of engagement of service provider shall be governed by bank's outsourcing policy.

Type of Service	Precaution
Standalone	1. SLA Should cover right to audit clause 2. Annual Audit report along with closure certificate by 3rd Party CERT-in empaneled firm for the data processing facility. 3. Annual Application audit report by 3rd Party CERT-in empaneled firm along with closure certificate. 4. Half-Yearly VAPT report along with closure certificate.
Bank Connected	1. SLA Should cover right to audit clause 2. Annual Audit report along with closure certificate by 3rd Party CERT-in empaneled firm for the data processing facility. 3. Half-Yearly VAPT report along with closure certificate.
Onsite	1. SLA Should cover right to audit clause 2. Periodic Audit report for due-diligence process of manpower recruitment along with closure certificate.

11.7 Compliance of Regulatory Guidelines

IS Audit will follow the guidelines/ advisories issued by regulator, Guidelines issued by Bank through various Circulars/ Compliance Dept. / Information Security Dept. while carrying out the IS Audit.

The major guidelines are given below:

RBI Guidelines viz Gopalkrishna Committee Recommendations, Cyber Security Framework in Banks, Master Direction on Digital Payment Security Controls, Storage of Payment System Data and Banks guidelines viz BCP, IRAC, Sharing of IT Resources etc. guidelines Issued by other regulatory bodies like NPCI & UIDAI regulatory guidelines if any will also be considered along with their updates.

12. Audit Report

The IS auditor is to provide a report, in an appropriate form to the intended recipients upon the completion of audit work. The report should identify the organization, the intended recipients and any restriction on circulation. The audit report is to state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed. The report is to state the findings, conclusions and recommendations and any reservations or qualifications or limitations in scope that the auditor has with respect to the audit. The IS Auditor should have sufficient and appropriate audit evidence to support the results reported. When issued, the IS auditor's report should be signed, dated and distributed according to the terms of the audit charter or engagement letter.

Where the IS auditor finds significant deficiencies in the control environment, the IS auditor should communicate these deficiencies to the General Manager / the Audit Committee of the Board and disclose in the report that significant deficiencies have been communicated.

The report should cover all the relevant points of observations with its implication, recommendations and Risk perception. All the recommendations are to be narrated in explicit and clear terms, which is implementable. The draft report is to be discussed with the user department as a prerequisite of exit interview and Management comments is to be obtained before concluding the audit process.

A typical audit report will include, among others, an introduction to the audit objectives, scope, general approach employed, and summary of the critical findings, the data to support the critical findings, potential consequences of the weaknesses, auditee's response and recommendations to rectify the weaknesses.

The audit reports need to be preserved with appropriate access controls for a period of 7 years from the date of receipt of management comments on the report. In case of overseas territories, the retention period would be as per the policy i.e., 7 years from the date of receipt of management comments or as per local regulatory requirement whichever is more stringent.

12.1 Compliance

The following generic guidelines to be followed for compliance timelines of IS Audit:
Clean Rectification Certificate (CRC) /Qualified Compliance Certificate (QRC)/ action taken along with evidences for closed observations and timeline of compliance for open observations should be submitted within 15 days to IS Audit Cell. In case of QRC, a Clean Rectification Certificate (CRC) should be submitted within 30 days of submission of QRC.

Criticality of observations is decided on the basis of likelihood of occurrence and business impact of findings

Sr.	Type of Systems audited	Criticality of Finding	Outer limit for management comments	Outer limit for compliance of Observations
1	Critical/ large applications/ infrastructures	High	5 days	30 days from submission of audit report
2	All other applications	Medium	7 days	45 days from submission of audit report
3	All others	Low	7 days	45 days from submission of audit report

 # Timelines are subject to change depending on the regulatory urgency.

12.2 Risk Acceptance

Top Management Steering Committee (TMSC) is authorised to grant or deny all requests for exceptions to the Information Security Policy. The Business owners and stake holders would need to conduct due diligence to mitigate the risk to an optimal level post which request for policy acceptation to be placed in TMSC. On approval the report with the final risk would need to be presented to the Audit Committee of Board in Coordination with A & I Department at HO and IS Audit Cell for the final acceptance of the risk.

13. Audit Follow-up

The IS auditor is to request and evaluate appropriate information on previous relevant findings, conclusions and recommendations to determine whether appropriate actions have been implemented in a timely manner.

If management's proposed actions to implement reported recommendations have been discussed with or provided to, the IS auditor, these actions should be recorded as a management response in the final report. Where management provides

information on action taken to implement recommendations and the IS auditor has doubts about the information provided, appropriate testing or other procedures should be undertaken to ascertain the true position or status prior to concluding follow-up activities. A report on the status of follow-up activities, including agreed recommendations not implemented, may be presented to the General Manager (Internal Audit). As a part of the follow-up activities, the IS Auditor should evaluate whether findings if not implemented are still relevant.

Follow-up activities by IS Auditors can be defined as a process by which they determine the adequacy, effectiveness and timeliness of action taken by Management on reported engagement observations and recommendations, including those made by external auditors and others.

A follow-up process should be established to help provide reasonable assurance that each review conducted by the IS Auditors provides optimal benefit to the organization by requiring that agreed outcomes arising from reviews are implemented in accordance with management undertakings, or that management recognizes and acknowledges the risks inherent in delaying or not implementing proposed outcomes.

Management should provide an implementation date when each proposed action is to be completed. When management's proposed actions to implement or otherwise address reported recommendations and audit comments have been discussed with or provided to the IS Auditor, these actions should be recorded as a management response in the final report with a committed implementation date.

14. Archival of Documents

IS Audit Cell should have an archiving / retention policy, in line with the Bank's Archival policy, to archive the audit results that:

- Ensures integrity of the data
- Defines appropriate access rights
- Decides on the appropriate archiving media
- Ensures ease of recovery

15. Outsourcing of IS Audit

The IS audit process may be outsourced when sufficient number of qualified IS auditor is not available in-house. In such a situation confidentiality of information is to be safeguarded by the service level agreement. Partial outsourcing of the internal IS Audit function to an external provider may be allowed considering the paucity of qualified people within the organization.

Outsourcing such audit services should be in accordance with the audit policy, it should be properly structured and professionally conducted and managed. There should not be any conflict of interest and it is to be confirmed that use of these services should not compromise independence. Potential conflict of interest may arise if the outsourced auditing firm performs IT audit function in addition to other audit services, such as providing the independent financial statement, or serving in an IT or management consulting capacity. IS audit Coordination committee is responsible for ensuring that the outsourced internal audit function operates effectively and complies with all regulations governing such arrangements. In all practical purpose the outsourcing should be partial with overall control and monitoring lies with internal IS audit Cell.

15.1. Using the work of other experts

The IS auditor should, where appropriate, consider using the work of other experts for the audit. He should assess and be satisfied with the professional qualifications, competencies, relevant experience, resources, independence and quality control processes of other experts, and prior to engagement. The IS 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.

The IS auditor should determine and conclude whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented. The IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts

does not provide sufficient and appropriate audit evidence. Wherever required he should provide appropriate audit opinion and include scope limitation where required evidence is obtained through additional test procedures.

The IS auditor should consider using the work of other experts in the audit when there are constraints that could impair the audit work to be performed or potential gains in the quality of the audit. An 'expert' could be an IS auditor from the external accounting firm, a management consultant, an IT expert or expert in the area of the audit who has been appointed by the top management or by the IS audit team. An expert could be internal to Bank or an external people.

The IS auditor should have access to all work papers, supporting documentation and reports of other experts, where such access does not create legal issues. Where the expert's access to records creates legal issues and hence such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert's work. The IS auditor's views/relevance/comments on adoptability of the expert's report should form a part of the IS auditor's report. If the IS auditor does not have the required skills or other competences to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the expert.

16. Job Rotation

As a matter of prudence, banks should rotate IS Auditors in a specific area on periodic basis, say at least once in two years.

17. Review of policy document

IS Audit policy is to be reviewed once in every 36 months and approved by the ACB / Board. Any new modified regulatory guidelines issued during review period will be incorporated in the IS Audit Policy on approval by the audit Committee of Board (ACB).

List of Abbreviations:

Acronym	Explanation
Bank	Uttar Pradesh Gramin Bank
ACB	Audit Committee of the Board
ACE	Audit Committee of Executives
CBS	Core Banking Solution
CISM	Certified Information Security Manager
CGEIT	Certified in the Governance of Enterprise IT
CEH	Certified Ethical Hawker
CQA	Certified Quality Analyst
COBIT	Control Objectives in information & Related Technologies
CIAD	Central Internal Audit Division
CISA	Certified Information System Auditor
CISSP	Certified Information Systems Security Professional
CISO	Chief Information Security Officer
CAAT	Computer Assisted Audit tools
CPE	Continued Professional Education
DISA	Diploma in Information System Auditor
ISACA	Information System Audit & Control Association
IS Audit	Information Systems Audit
NEFT	National Electronic Fund Transfer
RBI	Reserve Bank Of India

RTGS	Real Time Gross Settlement
RBIA	Risk Based Internal Audit
RBO	Regional Back Office
SW	Software
SITB	Specialized Integrated Treasury Branch
SWIFT	Society for Worldwide interbank Financial telecommunication
TBA	Total Branch Automation
CTS	Cheque Truncation System

Annexure: **List of Critical Applications**

Sr. No.	Application
1	2 Factor Authentication (2FA) - New
2	Bharat Bill Payment system (BBPS)
3	Bio Metric Authentication system
4	CBS
5	E- Banking (FEBA)
6	Internet Payment Gateway (IPG)
7	Mobile Banking
8	Real Time Gross Settlement (RTGS)
9	National Electronic Fund transfer (NEFT)
10	Unified Payment Interface (UPI)
11	Immediate Money Payment Solutions (IMPS)
12	BHIM Adhar pay (BAP)
13	Cheque Trancation system (CTS)
14	Debit Card Management System (DCMS)
15	Financial inclusion

Annexure-A

(I) **Suggested check list for the guidance of Auditor carrying out IS Audit**

I. Segregation of Duties

I.A. Are duties segregated between the data processing function and users?

a. Does the organizational structure provide for separation of functions between:
   i. Transaction initiation & authorization?
   ii. Console operations and data-entry?
   iii. Program team and Custody of System Documentation (including programs), confidential data, etc.?

b. Does the Data Base Administrator (DBA) / IS manager reports to higher authorities about day-to-day as well as non-routine activities?

c. Are data processing personnel restricted from having asset custodianship functions, and access to assets, particularly liquid assets?

I.B. Are the duties segregated within the IS functions?

(a) Does a current organization chart exist which defines the organizational structure within IS department/Computer Cell?
(b) Do current job descriptions exist for all personnel associated with IS department/Computer Cell?
(c) Are new employees provided with orientation upon recruitment?
(d) Have IS department/Computer Cell employees been provided with formal and on- the-job training to maintain knowledge, skills and ability in Information Technology and control-requirements?
(e) Is there a separation between Data Base Administration and other data processing functions?

I.C. Precautions regarding personnel involved in IS functions:

(a) Are employees who constitute a potential threat transferred or suspended immediately?
(b) Are references verified before an employee is recruited?
(c) Is the IS personnel (including DBA) required to take regular vacations, and are their duties reassigned during the vacation period?

II. Access Controls

II.A. Access controls: Is access to the main processor (i.e. system-console or server) adequately controlled?

a. Does the computer room have adequate physical barriers to prevent unauthorized access to the system console / server?
b. Are combination locks, security badges or other means used to restrict access to the computer server room, back-up storage library and documentation library?
c. Are combination locks, security badges or other devices changed periodically?
d. Has detective equipment been installed to monitor access to the computer server room, (or e.g. cameras with time and date stamp in case of ATM-Unit)?
e. Does the location of off-line storage of data, transaction journals and critical reports safeguard against unauthorized access?

II.B. Access controls: If access to programs and data including Data Centre / Disaster Recovery Centre is primarily controlled through passwords? Are procedures adequate?

a. Are password administration facilities in Operating System (OS) and in Application packages in vogue?
b. Is a security package in use or any other security facilities in O.S. and App. Packages being explored?
c. Is suitable security software installed and updated regularly in all systems for protecting software systems against virus, spyware, spam ware and other malicious programs?
d. Are various levels of passwords established for different transaction types, files and programs?
e. Are various levels of passwords required based on the usability, confidentiality and significance of information?
f. Are passwords periodically changed? How often passwords are changed?
g. Are all modifications to authorization tables and access privileges recorded and reviewed?
h. Are all Systems / Database logs validated by the Solution/Service provider at periodical intervals?
i. Are log-in IDs of terminated employees immediately disabled on the system?
j. Are users prohibited from selecting passwords that contain their names, or the passwords, which are very easy to guess?

k. If the DBA/password administrator assigns passwords first time, are delivery procedures appropriate to assure that an employee's password is not intercepted?

l. Does the employee change the password immediately after he receives from the DBA?

IIC. Access controls: If access to programs and data files is primarily controlled through physical restrictions in terminals, are procedures adequate?

a. Does the layout of the area where terminals are located prevent unauthorized access to equipment?

b. Do the location of terminals used for either data entry or inquiry; restrict access to authorized personnel when the system is in operation?

II D. Access controls: Are the programming activities properly controlled?

a. Do the procedures and system mechanisms prevent programmers from accessing production data, object programs and other automated procedures during the testing and debugging process?

b. Are programmers required to work on a separate computer system (i.e. other than production system)?

c. Is all live data removed from the computer system and secured in a separate library at the time software or hardware maintenance activities take place?

d. Does production software (i.e. Programs in use) protected from unauthorized access (i.e. use of a restricted facilities)?

e. Is all testing activity restricted to non-production programs and data?

f. Do the procedures used **FOR INCORPORATING NEW OR ALTERED PROGRAMMES IN PRODUCTION SYSTEMS**; prevent unauthorized access to other programs?

II.E. Access controls: Is system-activity appropriately monitored?

a. Does the computer system maintain a log of access activity?

b. Are invalid access attempts reported to, and investigated by management, DBA, and Computer Auditors?

c. Is the system capable of distinguishing activity source by terminal identification?

d. Is the system capable of identifying authorized individuals by multi-level passwords?

e. Are all entries by personnel restricted or secured areas recorded?

II.F. Access controls: Is hardware and software maintenance properly monitored/ controlled?

1. Do supervisory activities ensure that all hardware and software-maintenance is:

i. Identified?

ii. Authorized?

iii. Recorded?

iv. Reviewed?

v. Monitored?

II.G. Access controls: Is the operating system properly controlled?

a. Are the operating system options / configuration settings properly documented? b. Is the operating system free of extensive modifications?

c. Are the modifications in operating system configuration-settings subject to the same controls as application programs?

d. Does the data processing department have a system-software programmer on staff?

e. Are the patches/ upgrades / updates applied regularly on operating systems and other system applications?

II.H. Access controls: Distribution of Reports

a. Do the procedures for receipt and distribution of computer-outputs ensure that access to information is authorized?

b. Is a report distribution list used, for this purpose?

c. Do the waste disposal procedures include the destruction of obsolete reports, which contain sensitive data?

II.I. Access controls: Is access to blank cheques, demand drafts and other critical documents controlled?

a. Are these documents issued (internally to the concerned employee/s) on the basis of run schedules only?

b. Are these documents kept locked in a secure location when unattended?

c. Are records of supply of these forms maintained?

d. Are records of ACCESS TO supplies of these forms maintained?

e. Are these documents periodically inventoried?

f. Are the documents pre-printed?

g. Are the documents pre-numbered or sequentially numbered and accounted for?

II.J. Access controls: Is there other access controls in place in the following areas?

a. Are all computer language-compilers removed from the production system, (and at the location of software development site, protected from unauthorized access)?

b. If the computer system uses an interpreter of the language, have adequate measures been taken to prevent the illegal interrupt of program execution or alteration of program logic by computer operators?

c. Are report-generation packages secured from the update capabilities (especially from modifying the contents of the reports generated)?

d. Do the reports generated clearly identify their source?

e. Is the availability of utilities, which can be used to alter or copy data and programs restricted and controlled?

III. Authorization

III.A. Authorization: Does the senior management or a committee authorize the following IS-related functions?

a. IS Personnel Policy?
b. Hardware Policy?
c. Software Policy
d. Software Development Policy?
e. Programming Methodology?
f. IS Security Policy?
g. Documentation Policy?
h. Information Policy?
i. Priorities of IS-related activities?
j. Major system / design /equipment changes?
k. Manpower allocations by project?
l. Procedures for security and control measures?
m. Research and Development studies?
n. IS budgets?
o. IS long-range plans?

III.B. Authorization: Are only authorized transactions processed, and unauthorized transactions (if any) identified?

a. Are clerks / computer-operators provided an approval-form to assure authorization (in addition to on-line authorization), in order to process the transactions?

b. Does the computer system verify authorization for transactions entered on-line, through terminal identification? (i.e. a data-entry terminal cannot be used simultaneously as authorization terminal).

c. Are individuals held accountable for all transaction-activities through the use of transaction - logs?

d. Do the transaction logs contain the log in-id, the source (i.e. terminal #), Voucher #, Date & time of transactional for ALL the transactions during on-line data-entry?

e. Are permanent records of ALL the live programs and data on the computer system (in the following areas), maintained by System Administrator as well as Branch Manager?

i. Production (i.e. live) files and directories?
ii. Production program libraries?
iii. Production environment parameter settings (e.g. O.S. and DBMS configuration settings)?

III.C. Authorization: Are written standards developed / prepared to provide management's general and specific authorization for various IS-related activities?

a. Is a written manual of systems and procedures available for all computer operations, and does it provide a definition and explanation of management's general and specific authorization to process transactions?

b. Are there written standards for:
i. Hardware selection?
ii. System Software selection?
Iii. Application package selection?
iv. Network component selection?
v. System design and development?
vi. Programming standards?
vii. Testing?
viii. Program approval standards?
ix. Implementation (including procedures for putting a program/system into production)?
x. Hardware and especially Software Change Management Procedures?

III.D. Authorization: Is system development properly controlled?

a. Is a formal System Development approach used? (Please specify):
b. Does management make a clear distinction between production (i.e. Live) and development programs?
c. Is "prototyping" done?
d. Do the procedures for system design, including the acquisition of software packages require active participation by representatives of users, accounting, internal audit, and computer auditors (I.S. auditors), as appropriate?
e. Does each system have a written (in detail) specification, which are reviewed and approved by management, and applicable users before preparation of the detailed systems design specifications to assure implementation of an acceptable quality standards?

III.E. Authorization: Are new systems adequately tested?

a. Do software-testing a joint effort of programmers, system developers, computer (I.S.) - auditors, and users?
b. Does system testing include testing of both, the manual and computerized phases of the system?
c. Is test data developed to specifically test the functioning of programmed control procedures?
d. During parallel testing, is consideration given to whether errors exist in the populated data, to test programmed controls?
e. Is documentation of system tests (data and results) retained for future use, which will be required in case of later system modifications?
f. Are test results reviewed and approved by user / management personnel before authorizing the transfer of programs into the live environment?
g. Do final testing procedures provide user, management, IS-staff and IS-audit personnel with a clear identification of the program version used to perform the test?
h. Are programmers prohibited from using live data files to test programs?

III.F. Authorization: Is system conversion adequately planned and controlled?

a. Are formal, written conversion procedures prepared?
b. Is formal approval by system development steering - committee / management and IS auditor obtained, of IS related activities including a review of changes from original design specifications, review of system test results, review of input and output controls, and review of documentation prior to putting a new system into production?
c. Are these written conversion procedures approved by management, internal audit, IS auditing, user departments and accounting personnel as appropriate?
d. Are all master file / table and transaction file / table conversions controlled to prevent unauthorized changes, to provide accurate and complete results, and to ensure data integrity? e. Do program transfer - procedures ensure that only those programs, which were used for the final test, are transferred to the live environment?

f. Are control totals such as record counts and hash total established to allow reconciliation of converted files to the original manual or computer files?
g. Are critical matter files / tables printed before and after conversion (e.g. deposits file, payroll master file / table, central information table / file, etc.)?
h. Does someone without incompatible duties compare the before and after details of these critical matter files / tables?

III.G. Authorization: Are program changes authorized?

a. Do policies and procedures for initiating changes to programs and other forms of processing logic ensure that management authorizes all changes?
b. Do policies, procedures and mechanisms ensure that personnel responsible for application program perform no changes to the operating system configuration?
c. Is a log maintained of all changes requested that identify the person initiating the change, the date initiated and the date implemented?
d. Does this log also identify the specific program (s) and / or operating procedures affected by the change?

III.H. Authorization: Are program changes monitored and controlled?

a. Do procedures ensure that all changes to the system are documented?
b. Are program modifications made ONLY TO COPIES OF current production programs rather than the programs themselves?
c. Does a responsible official INDEPENDENT OF PROGRAMME authorize operations personnel to put a modified program into production?
d. Are source programs supplied when program changes are authorized for putting into live operation?
e. Is the following documentation obtained / prepared before and after each change, and retained as a permanent record? i. Files / directories in the system? ii. Production library directories? iii. Program source listings? iv. Operation procedures' listings? v. Systems flowcharts? vi. Data flow diagrams? vii. Entity Relationship (ER) diagrams?
f. Are operations' procedures updated to reflect system changes?
g. Do system administrators of all transfers to production libraries (i.e. live environment) maintain logs?
h. If patching techniques are used:
i. Are they allowed only in emergencies?
ii. Are they allowed only after supervisory approval?
iii. Are records of patches maintained, including appropriate approvals, records of the instructions / routines altered, the name of the person making the changes and the reason for the changes?

IV. Supervision and Review

IV.A. Supervision and review: Are IS related activities subject to review by management?
a. Is management knowledgeable about the activities performed by the computer system and the methods used for operation and maintenance of the system?
b. Are logs of computer processing and balancing activities available, and reviewed by Management at least on half-yearly basis.
c. Are logs the basis for preparation of performance statistics to be reviewed by management?
d. Are logs the basis for charging computer expenses to user departments, (if applicable)?
e. Is the system log file / table properly controlled to prevent unauthorized changes?
f. Are all reports of reprocessing activity retained, reviewed by supervisory personnel and is computer time accounted for?
g. Is computer processing scheduled, either manually or through automated techniques, and regularly compared to machine utilization reports and / or console logs?

h. Does the processing schedule include periodic (i.e. daily, fortnightly, month-end, quarterly, six-monthly, yearly, exceptional etc.) processing-requirements?
i. Are significant variations from scheduled processing investigated?

IV.B. Supervision and review: Does the management periodically review access - authorization?
a. Are authorization levels for terminal users and points of transaction / operation organization periodically reviewed?
b. Do supervisory or managerial personnel routinely review the logs and reports of invalid access attempts?

IV.C. Supervision and review: Are computer operations well documented and organized in an orderly fashion?

a. Is computer operations staff (including DBAs / System Administrators, and computer auditors) adequately trained to the extent necessary to perform all their tasks in a systematic manner (without relying upon external personnel)?
b. Do computer processes detect or prevent the initiation of processing steps, which are OUT OF SEQUENCE?
c. Are hardware maintenance boundaries contractually defined with each vendor when the bank (or even a branch / office within a bank) uses hardware from more than one manufacture?
d. Is a record of all Hardware problems (including UPS) properly maintained in a register?
e. Is a record of all Software problems properly maintained in a register?
f. Is preventive maintenance routinely performed? How frequently?
g. Is a record of such maintenance prepared and reviewed?
h. Is the use of off-line data files for processing, controlled through verification by the system, before the processing is initiated?

IV.D. Supervision and review: Has management established documentation standards to allow for maintenance and supervision of IS-related activities in the following areas:

a. Information Systems setup documentation (at each location)?
b. Systems documentation?
c. Program documentation?
d. Operations documentation?
e. User documentation (e.g. user profile and the kind of operations he is allowed to perform)?
f. Do supervisors review "Users" and "Technical" manuals to make sure that prescribed documentation standards are adhered to?
g. Are "documentation standards" and "change procedures" adequate to ensure that documentation is maintained in a correct and consistent manner?

IV.E. Supervision and review: Does adequate and up-to-date system- documentation exist (for every system) including the following:
a. Systems narrative?
b. Systems flowcharts?
c. Broad input-design?
d. Broad Database design?
e. Broad (context-level) DFDs i.e. Data Flow Diagrams?
f. Data element definitions?
g. Codes Design?
h. Dialogue Design?
i. Broad Procedure-Design?
j. Held Design?
k. Broad Output Design (Report and Screen Design)?
l. Data capture procedures?
m. Backup and recovery procedures?
n. System changes?

IV.F. Supervision and review: Does adequate and up-to-date documentation exist including the following:

a. Detailed System Flowcharts?
b. Narrative description of each major program module, subsystem?
c. In-detail program-flowcharts?
d. In-detail DFDs (Data Flow Diagrams)?
e. Decision tables?
f. In-detail database design?
g. In-detail ER diagrams?
h. List of constants, codes and tables used?

Source program listing?

- Operating System (OS) Commands listings? Specimen vouchers?
- Specimen data-entry (and other interface) screens?
- Specimen reports?
- Program changes?
- Changes in ANY COMPONENT of the system?

IV.G. Supervision and review: Are computer jobs streams supported by computer set-up and run instructions including:

- Set-up instructions and device assignments?
- Identity of input and output data tables/files?
- Parameters of Job Control Language /OS Commands?
- Normal console/server-messages for each run?
- List of error and halt messages, probable causes, programmed and machines halts, and required action?
- Restart and recovery procedures?
- Estimated run times and maximum run time (for every major job /major task)?
- Form (and distribution) of printed and other outputs? End of job instructions?
- Output destination and retention instructions?

IV.H. Supervision and review: Are procedures for input and output documented?

Are input procedures documented to describe all tasks necessary for the control of transactions processed by the system including:

i. Input receipt?
ii.Data entry?
iii.Error correction?
iv. Source document control?
v. Permanent record retention?

Are procedures documented for the generation, verification and distribution of computer output including:

i. Output reports generation?
ii. Report balancing and reconciliation?
iii.Report distribution?
iv. System inquiries?

Are control totals produced by the system to allow balancing with input control totals including:

i Batch number?
ii. Amount totals of significant fields?
iii.Hash totals of significant fields?
iv. Transaction or record counts?
v. Ending number of master file records?
vi Total number of master file / table records?

V. Security and recovery

V.A. **Security and recovery: Has the potential risk of events, which could cause short-term or sustained loss of computer-processing capability, been identified?**

- Has the maximum time period, for which loss of computer processing could be tolerated without serious disruption to the business, been identified (separately for every business-operation based on nature and criticality of that business operation)?
- Has the effect of loss at differing times i.e. start of day, peak business-hours time, end of week, end of month, end of year etc.), been addressed?
- Have the effects of daily operating practices, customer reaction, and exposure to loss been considered?
- Has the effect of loss of individual components of the system (Hardware components, network components, system and application Software components, data, documentation, people etc.) been isolated?

V.B. **Security and recovery: Has Information Systems activities related insurance coverage been considered for the following risks:**

- Equipment destruction?
- Programme or software destruction?
- Loss of data?
- Business interruption?
- Errors of omissions?
- Fidelity insurance on IS personnel?
- Payment for use of alternative equipment?
- Annual management review and approval of IS activities related insurance coverage?

V.C. **Security and recovery: Do the plans and procedures exist to prevent a short-term or partial failure in a controlled manner?**

- Does the environment for the computer systems conform to manufacturer's specifications for electrical, humidity, temperature and air particle tolerance?
- Does the physical location of computer equipment discourage access or interruption by unauthorized personnel and reduce vulnerability to environmental effects and natural disasters? Does the on-premises backup-storage area provide reasonable protection against accidental damage or destruction of data, programmes and documentation?
- Does the bank have written policies and procedures for backup and recovery of all data and programmes stored on magnetic media, to assure sufficient backup exists to restore them if they are destroyed?

V.D. **Do the plans and procedures exist to recover from a short-term or partial system failure in a controlled manner?**

- Do procedures exist for recovery in an orderly manner in the event of processing interruptions resulting from such occurrences as equipment malfunction, power fluctuations, software error or loss of on-line data?
- Is there procedure for continuation of processing in the absence of key individuals (IS persons) within the branch/office?
- Are programmes, which have backup data, included in the routinely run application software, so that the backup procedure will not be a DBA's or operator's choice?
- Is at least one current copy of the supervisory and application programme library maintained in the nearby magnetic-storage-library, as immediate backup?
- Are error-recovery procedures for short-term failure tested periodically to ensure control of the process?
- How frequently?
- Are computer operators' duties rotated periodically, to have internal controls, and also to ensure the availability of trained backup staff?
- Is the "Maker-Checker" principle used in Software development activities also?

V.E. Security and recovery: Are backup procedures adequate?

- Are current copies of the following maintained off-site?
  i. Operating systems?
  ii. Source programmes?
  iii. Runtime (executable) codes?
  iv. Master data?
  v. Transaction data necessary for recovery?
  vi. Programme documentation?
  vii. Operating instructions?
  viii. Critical forms and supplies?
  ix. Disaster recovery plan?
  x. System documentation?
- When "backup copies" of programmes are used, are they duplicated before being put into production?
- When backup copies of master or transaction data are used, are they duplicated before being put into production?
- Are restoration / recovery procedures tested periodically, after having secured backup copies of all data, software, and documentation and transaction sources?
- How frequently?

V.F. Security and recovery: Are the arrangements with vendors adequate?

- Are vendors responsible for reliable hardware and software support to avoid the possibility of processing interruption due to lack of support?
- Do remedial equipment - maintenance arrangements provide for response to problems in sufficient time to prevent business disruption?
- What is the average response time after registering the complaint?
- Does the equipment maintenance vendor maintain an inventory of replacement components (which are frequently required for local service)?

V.G. Security and recovery: Is the disaster recovery planning adequate?

- Is there a detailed disaster recovery planning explaining procedures and steps necessary for recovery after the disaster?
- Is a copy of the plan stored off premises or in a location where it would not be destroyed in the event of a disaster?
- Have backup alternatives been considered (i.e. Hot site, cold site, warm site, reciprocal arrangements, etc.)?
- Are alternative computer equipment arrangements tested periodically to ensure that the plan functions?
- has the disaster recovery plan been tested?
- How frequently?

V.H. Security and recovery: Is other recovery - considerations adequate?

- Do documented operating procedures permit continuation of computer processing in the event of permanent loss of key operations personnel?
- Does the documentation of the system permit maintenance by alternate support personnel in the event of loss of key programmers?
- Does the Disaster Recovery Plan (DRP) include the provision for continuation of business operations in the event of any (minor or major) disaster?
- Is the bank (i.e. every computerized branch and office) in compliance with the regulatory / statutory requirements, with respect to retention of data, generate reports which is in the machine-readable form?

Annexure B

IS Audit Scope

The indicative scope of IS Audit is given below :

* Alignment of IT strategy with Business strategy
* IT Governance related processes
* Long term IT strategy and Short term IT plans
* Information security governance, effectiveness of implementation of security policies and processes
* IT Architecture
  - Acquisition and Implementation of Packaged software
    - > Requirement Identification and Analysis
    - > Product and Vendor selection criteria
    - > Vendor selection process
    - > Contracts
    - > Implementation
    - > Post Implementation Issues
  - Development of software - In-house and Out-sourced
    - > Audit framework for software developed in house, if any
    - > Software Audit process
      - o Audit at Program level
      - o Audit at Application level
      - o Audit at Organizational level
    - > Audit framework for software outsourcing
  - Operating Systems Controls
    - > Adherence to licensing requirements
    - > Version maintenance and application of patches
    - > Network Security
    - > User Account Management
    - > Logical Access Controls

- > System Administration
- > Maintenance of sensitive user accounts

- Application Systems and Controls
  - > Logical Access Controls
  - > Input Controls
  - > Processing Controls
  - > Output Controls
  - > Interface Controls
  - > Authorization Controls
  - > Data Integrity / File Continuity controls
  - > Review of logs and audit trails
- Database Controls
  - > Physical access and protection
  - > Referential Integrity and accuracy
  - > Administration and Housekeeping
- Network Management audit
  - > Process
  - > Risk acceptance (deviation)
  - > Authentication
  - > Passwords
  - > Personal Identification Numbers ('PINS')
  - > Dynamic password
  - > Public key Infrastructure ('PKI')
  - > Biometrics authentication
  - > Access Control
  - > Cryptography
  - > Network Information Security
  - > E-mail and Voicemail rules and requirements
  - > Information security administration
  - > Microcomputer / PC security

- > Audit trails
- > Violation logging management
- > Information storage and retrieval
- > Penetration testing

- Physical and environmental security
- Maintenance
  - > Change Request Management
    - o Software developed in-house
  - > Version Control
  - > Software procured from outside vendors
  - > Software trouble-shooting
    - o Helpdesk
  - > File / Data reorganization
  - > Backup and recovery
    - o Software
    - o Data
    - o Purging of data
  - > Hardware maintenance
  - > Training
- Internet Banking
  - > Information systems security framework
  - > Web server
  - > Logs of activity
  - > De-militarized zone and firewall
  - > Security reviews of all servers used for Internet Banking
  - > Database and Systems Administration
  - > Operational activities
  - > Application Control reviews for internet banking application
  - > Application security
- Privacy and Data Protection

- > Controls established for data conversion process
- > Information classification based on criticality and sensitivity to business operations
- > Fraud prevention and Security standards
- > Isolation and confidentiality in maintaining of Bank's customer information, documents, records by banks
- > Procedures for identification of owners
- > Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
- > Media control within the premises

- Business Continuity Management
  - > Top Management guidance and support on BCP
  - > The BCP methodology covering the following :
    - o Identification of critical business
    - o Owned and shared resources with supporting function
    - o Risk assessment on the basis of Business Impact Analysis ('BIA')
    - o Formulation of Recovery Time Objective ('RTO')and Identification of Recovery Point Objective ('RPO')
    - o Minimising immediate damage and losses
    - o Restoring of critical business functions, including customer-facing systems and payment settlement systems
    - o Establishing management succession and emergency powers
  - > Addressing of HR issues and training aspects
  - > Providing for the safety and wellbeing of people at branch or location at the time of disaster
  - > Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
  - > Independent Audit and review of the BCP and test result
  - > Participation in drills conducted by RBI for Banks using RTGS / NDS / CFMS services
  - > Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers

- Asset Management
  - > Records of assets mapped to owners
  - > For PCI covered data, the following should be implemented :
    - o Proper usage policies for use of critical employee facing technologies
    - o Maintenance of Inventory logs for media
  - > Restriction of access to assets through acceptable usage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labelling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
  - > Review of duties of employees having access to asset on regular basis.
- Human Resources
  - > Recruitment policy and procedures for staff
  - > Formal organization chart and defined job description prepared and reviewed regularly
  - > Proper segregation of duties maintained and reviewed regularly
  - > Prevention of unauthorized access of former employees
  - > Close supervision of staff in sensitive position
  - > People on notice period moved in non-sensitive role
  - > Dismissed staff to be removed from premises on immediate effect
- IT Financial Control
  - > Comprehensive outsourcing policy
  - > Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security lapse in the vendor contract
  - > Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  - > Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information / records within reasonable frame of time.
- IT Operations
  - > Application Security covering access control
  - > Business Relationship Management
    - o Customer Education and awareness for adaptation of security measures

- o Mechanism for informing banks for deceptive domains, suspicious emails
- o Trade marking and monitoring of domain names to help prevent entity for registering in deceptively similar names
- o Use of SSL and updated certification in website
- o Informing client of various attacks like phishing

> Capacity Management

> Service Continuity and availability management

- o Consistency in handling and storing of information in accordance to its classification
- o Securing of confidential data with proper storage
- o Media disposal
- o Infrastructure for backup and recovery
- o Regular backups for essential business information and software
- o Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
- o Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
- o Avoidance of single point failure through contingency planning

> Service Level Management

- Project Management

> Information System Acquisition, Development and Maintenance

- o Sponsorship of senior management for development projects
- o New system or changes to current systems should be adequately specified. programmed, tested, documented prior to transfer in the live environment
- o Scrambling of sensitive data prior to use for testing purpose

> Release Management

- o Access to computer environment and data based on job roles and responsibilities
- o Proper segregation of duties to be maintained while granting access in the following environment -
  -- Live

-- Test

-- Development

o Segregation of development, test and operating environments for software

Record Management

o Record processes and controls

-- Policies for media handling, disposal and transit

-- Periodic review of Authorization levels and distribution lists

-- Procedures of handling, storage and disposal of information and media

-- Storage of media backups

-- Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement

Technology Licensing

o Periodic review of software licenses

o Legal and regulatory requirement of Importing or exporting of software

IT outsourcing related controls

Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes

Data Centre operations and processes

Review relating to requirements of card networks (for example, PIN security review)

****