	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

1. Introduction:

Technology adoption by Banks and Financial Institutions has increased significantly in recent times and technological innovation has become key tool to drive the financial services to the unreached population. In order to maintain transparency and safety in the banks in delivering services to rural mass and also to mitigate the risks emanating from adoption of technology, there is an imperative need to introduce Information system (IS) Audit in the Bank.

Information system audit is the process of collecting and evaluating evidence to determine whether the information system safeguards assets, maintains data integrity, achieves organisational goals effectively and efficiently keeping in view of the IT Policy of the Bank.

2. Objectives:

It is essential for the Bank to ensure that it's Systems Assets/Resources and IT Processes are dependable, controlled and protected from misuse at all times. As part of the confirmatory process, it follows that all IT systems are audited at periodic intervals and a report on their status are submitted to Audit Committee of the Board.

Major objectives of the Information Systems Audit are as under:


- a. Safeguarding Information Systems Assets/Resources and IT Processes.
- b. Verification of Data Integrity and Security.
- c. Evaluation of System effectiveness and efficiency.
- d. Verification of compliance to Internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

a. Safeguarding Information Systems Assets/ Resources and IT Processes:

- I. Monitoring effective usage of Hardware, software, networking & communication facilities, people (Knowledge), system documentation, supplies etc.
- II. Evaluation of infrastructure (like Power, Air Conditioning, Humidity Control, physical security, Surveillance and monitoring, Incident monitoring etc.) in safeguarding of IS Assets/Resources.

b. Verification of Data Integrity and Security:

Validate that the data entered and captured in the system is duly authorized, verified and completed and that proper control is exercised at all stages viz. Data preparation, Input, verification, output, modification, deletion, electronic transmission, etc. to ensure authenticity and correctness of data.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

c. Evaluation of System effectiveness and efficiency:

Evaluate the extent to which the organizational goals, business and user needs have been met with and to determine whether resource utilization is effective and efficient in achieving the desired objectives.

d. Verification of compliance to internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

- i. Evaluate the level of compliance on adherence to maintenance of Integrity, Confidentiality, Reliability, Availability and Dependability of Information resources;
- ii. Legal, Regulatory and Statutory requirements.
- iii. Internal Policy and Procedures based on prescribed standards and guidelines.


3. Scope of IS Audit:

The scope of IS Audit Includes:

- a. Determining effectiveness of planning and oversight of IT activities.
- b. Evaluating adequacy of operating processes and internal controls
- c. Determining adequacy of enterprise – wide compliance efforts, related to IT policies and internal control procedure.
- d. 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.

4. IS Audit Methodology:

- i. Identify the risks that the organization is exposed to, In the existing computerized environment and to prioritize such risks for remedial action.
- ii. Whether the implementation of Information Technology in the organization is as per the parameters laid down in the Information Security Policy and as duly approved by the Board of Management.
- iii. Verify whether the Information systems policies have been devised covering various information assets for the entire organization and that the organization's systems and procedures and laid down IS security policies are adhered to.
- iv. Verify whether the checks and balances prescribed by IS security policy and other relevant guidelines are strictly adhered to / complied with, towards risk

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

mitigation through proper maintenance and prevention of abuse /misuse of IT assets and computer crimes.

- v. Verify and comment on the level of checks and balances for ensuring compliance of laid down control measures.
- vi. Adhere to the established norms of ethics and professional standards to ensure quality and consistency of audit work.

5. IS Audit Setup:

5.1 IS Audit Function:

Internal Audit is a part of the Board's assurance process with regard to the integrity and effectiveness of systems and controls.


Critical Components and Processes:

IS Audit being an integral part of the Internal Audit, auditors will also be required to be independent, competent and exercise due professional care.

Independence: IS Auditors should act independently of the bank's management. To ensure the tasks performed fulfil bank's overall audit objective while preserving its Independence, objectivity and competence of IS Audit function (Inspection Department) from other departments and offices, its personnel shall report to AGM, IS Audit Cell. AGM, IS Audit Cell will report to General Manager (DoS), who shall report to the Audit Committee of the Board through Chief Executive Officer

The Inspection department shall be independent of the activities audited. The IS audit cell and IS Security Cell should be managed by two different sections to avoid conflict of Interest, under different controlling authorities/ General Managers.

In matters related to the audit, the IS Audit should be independent of the auditee, both in attitude and appearance. The Audit Charter or Policy, or engagement letter (in case of external professional service provider), should address independence and accountability of the audit function. In case independence is impaired (in fact or appearance), details of the impairment should be disclosed to the Audit Committee or Board. Independence should be regularly assessed by the Audit Committee. In case of rotation of audit staff members from IT department to the IS Audit, care should be taken to ensure that the past role of such individuals do not impact their independence and objectivity as an IS Auditor.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

Competence: IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience. They should be appropriately qualified, have professional certifications and maintain professional competence through professional education and training. As IT encompasses a wide range of technologies, IS Auditors should possess skills that are commensurate with the technology used by the bank. They should be competent audit with sufficient professional skills and relevant experience. Qualifications such as CISA/DISA/CISSP, along with two or more years of IS Audit experience, are desirable. Similar qualification criteria should also be insisted upon, in case of outsourced professional service providers.

Due Professional Care: IS Auditors should exercise due professional care, which includes following the professional auditing standards in conducting the audit. The IS Audit Head should deal with any concerns in applying them during the audit. IS Auditors should maintain the highest degree of integrity and conduct. They should not adopt methods that could be seen as unlawful, unethical or unprofessional to obtain or execute an audit.

Outsourcing related to IS Audit:


The Bank may decide to outsource execution of segments of audit plan to external professional service providers, as per the overall audit strategy decided in co-ordination with General Manager (DoS) & Audit committee.

The work outsourced shall be restricted to execution of audits identified in the plan. Bank will ensure the overall ownership and responsibility of the IS audit including the IS Audit planning process, risk assessment and follow-up of compliance remains within the bank.

Both the General Manager (DoS) and Audit Committee should ensure that the external professional service providers appointed should be competent in the area of work that is outsourced and should have relevant prior experience in that area.

Composition of IS Audit committee:

1. General Manager (IT) – Member
2. General Manager (DoS) –Member
3. Chief Information Officer (CIO) – Member

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

4. Concurrent auditor, PDCCB – Member
5. Dy. General Manager (DoS) – Convenor

5.2 Audit charter or policy:

Audit charter or policy is a document which guides and directs activities of an internal audit function. The responsibility, authority and accountability of the information systems audit function has to be appropriately documented in the engagement letter clearly defining the responsibility, authority and accountability of the IS audit function, for outsourcing of IS Audit.

The responsibility and accountability of internal IS auditors will be the same, as applicable to general Inspecting officials as per the prevailing Internal Inspection/audit guidelines.

5.3.1 Responsibilities:


The primary responsibility of the IS Audit is to achieve the objectives of the IS Audit function. In brief, the responsibilities of IS Audit function of the Bank is to:

1. Identify and assess potential risks to the Bank's operations.
2. Assess the means of risk mitigation and safeguarding of IT assets.
3. Review the adequacy of controls established, to ensure compliance with the policies, plans, procedures and business objectives.
4. Assess the level of compliance to the established procedures / controls.
5. Assess the reliability and security of financial management Information and the systems and operations that provide this information.
6. Assess the level of utilization of IT resources to understand their efficient and effective use for business growth.

5.3.2 Authority:

The Inspection Department / System, in the course of its IS Audit activities is authorized to have unrestricted access to all areas of the bank, activities, documents, records, Information, properties and personnel etc. relevant to the performance of IS Audit function.

All members of staff and Management to supply such Information and explanations as may be needed within a reasonable period of time to IS Audit staff.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

Heads of Department/Branches should inform Inspection department/ system without delay of any significant incident concerning security and / or compliance with regulations and procedures.

5.3.3 Accountability

The Inspection Department shall prepare annual plan for IS audit along with RBIA (regular Inspection), covering all the computerized environments of the Bank Viz. Branches / Offices /Departments etc., as per the periodicity prescribed in the Inspection & Audit Policy document.


Segmented risk profiling of IT Resources/Processes/Infrastructure are to be made by CISO, in consultation with CIO, covering all critical Assets to begin with. Based on the risk profiling / risk assessment provided by CISO, IS Audit Cell shall prepare scope of work document and Risk Based IS Audit (RBIA) Plan, covering all critical IS Assets used in CBS environment.

The plan covering, IS Audit of Branches/Offices/Departments/Critical Resources approved and finalized by the General Manager (DoS) shall be placed for approval/adoption by ACB.

In case of need, General Manager (DoS) may make modifications to the approved plan based on the exigencies and keep ACB apprised of such modifications.

The IS Audit Cell of Inspection Department is responsible for deciding on the scope/Timing of IS Audits and in finalization/ Implementation of IS Audit Plan. IS Audit covering Branches/Offices/Departments will be implemented by IS Audit Cell.

However, IS Audit of Critical Resources may be carried out by utilizing the services of External Resources, (wherever required in case Professional / Technological expertise is not available internally). The IS Audit Cell, Inspection Department shall coordinate with External IS Auditors whenever their services are engaged for any IS Audit activity in the Bank.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

IS Audit Cell shall ensure strict adherence of timely audit of Information system resources as per the approved plan. CISO, IS Audit Cell shall place a periodic review report on the compliance to the findings of IS audit to ACB and follow up the directions/observations of ACB for further compliance.

5.4 Organizational Structure: IS audit being an integral part of internal audit, requires an organisational structure with well-defined roles which needs to function in alignment with the internal audit and provide technical support on key focus areas of audit.

5.4.1 Board of Directors to manage the complexity of IS Audit Oversight. A designated member of the Audit Committee needs to possess the relevant knowledge of Information Systems, IS Controls and IS Audit issues. The designated member should also have relevant competence to understand the ultimate Impact of deficiencies identified in IT Internal Control framework by the IS Audit function. The Board or its Audit Committee members should be Imparted training to fill any gaps in the knowledge related to IT risks and controls.

5.4.2 Functions of ACB on IS Audit related areas: The Audit Committee should devote appropriate and sufficient time to IS audit findings identified during IS Audits and members of the Audit Committee would need to review critical Issues highlighted and provide appropriate guidance to the Bank's management.


5.4.3 Bank shall have an exclusive Cell, IS Audit Cell, with IS Audit function within the Inspection Department led by an IS Audit Head (CISO), assuming responsibility and accountability of the IS audit function, reporting to the Chief Information/Technology Officer (CTO/CIO).

5.4.4 Wherever the bank uses external resources for conducting IS Audit in areas where the required expertise / professional skills are lacking within the bank, the responsibility and accountability for such external IS audits shall remain with the IS Audit Head - CISO.

6 Administration of IS Audit:

6.1 Conduct of Audit:

Information System Audit of branches / Offices/ Department shall be carried out as per the prescribed periodicity. IS Audit being a specialized job, the scope and function of IS Audit Cell shall be limited to organizing /conducting

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

audit of Information and Communication Technology Infrastructure used by the bank, follow up with CISO/IS Security Cell etc. for timely rectification of the deficiencies.

6.2 System of IS Audit:

The IS Audit Policy covers all the computerized Departments/Offices of the Bank including CBS Project Office / Data Centre, DR Site for CBS/ATM, Branches under Core Banking Solution, Service Branches, ATM Switch /ATM Service Centre, ATMs, Treasury Department, Electronic Payments Department, HRM Department, NEFT/ RTGS Cell, Registering Authority (Digital Certificate) etc. and any other new information technologies to be Implemented by the Bank from time to time. In short, it includes all the activities/areas of the organization, where IT systems are used for business purpose.

The methodology adopted for IS Audit / Computer Audit includes a blend of input-output report reconciliation, interview and interaction with the concerned IT users/ IT personnel, verification of reports / registers maintained both manually as well as in the system.

6.3 Conduct of IS Audit of CBS application and Delivery channels by CISO:


IS audit of CBS application and Delivery channels at HO level is of specialized nature requiring technical expertise /specific skill / additional tools. Specific audit tools (CAAT) may be Introduced / used in addition to other audit techniques like "audit through the computer" and "audit with the computer", so as to timely identify and plug vulnerable areas in safeguarding IT assets, by way of risk mitigation for the audit of IT resources.

The team of IS auditors shall be exposed to the use of Computer Assisted Audit Tools (CAAT) and related system tools in carrying out the IS audit.

The audit emphasizes on determining the level of compliance with laid down policies, systems and procedures.

6.4 Role of IS Audit Cell:

1. IS audit Cell at Head Office is established under the overall control of Inspection Department for organizing and follow up of IS Audit activities of

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

the bank. The wing shall be manned by CISA/DISA/CISSP qualified IT Officers of the Bank in addition to officers with Information Technology experience. The term of these Officers shall be limited to a period of 5 Years. They shall be periodically provided with necessary training (class room as well as on the job) to update/upgrade their IT knowledge and skills to conduct IS audit using audit tools (CAAT) and testing accelerators which will enable them to effectively carry out the job assigned to them.

2. CISO shall follow up for rectification of deficiencies and submit Action Taken Report (ATR)/ steps initiated as risk mitigation measure to IS Audit Cell within 15 days of the report of observations of IS Audit.
3. IS Audit Cell shall continue to function independent of ITD and IS Security Cell but work in co-ordination with them. IS Audit being a specialized job, the scope and function of IS Audit Cell shall be limited to auditing of the computer based information systems and shall not include financial/transactional audit.
4. IS audit cell shall monitor the compliance to various IT guidelines/ RBI/legal/statutory requirements by various wings of the organization that are making use of IT assets. The follow up and placement of reports will be carried out as per the Internal guidelines.


6.5 External IS Audit firms:

The Bank may consider engaging the services of accredited External IS Audit firms for IS Audit of Branches / Offices / IT Infrastructure Including Network Audit, software audit, Vulnerability Assessment, etc. to meet any Business /Statutory requirements. Depending on the nature and criticality of assignment, the Bank may stipulate eligibility criteria of the External IS Audit firms, fees payable etc. The engagement letter should cover the scope of IS Audit, objectivity, duration etc. apart from addressing the areas of responsibility, authority, and accountability.

7. IS Audit Policy Guidelines:

7.1 General

The checklist based IS audit shall cover all the computerized branches / departments / offices of the bank. The checklist based IS Audit of Branches

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

(including new branches opened/ to be opened) shall be carried out along with regular Inspection of the Branch and IS audit rating arrived shall be dovetailed in to RBIA format, as spelt out under Rating System (Para 8.1 of this Policy).

7.2 Critical Success Factors:

The following critical factors are important for successful implementation of the IS Audit Policy.


1. Posting of IT Officers to Inspection System - Officers, who have at least 3 years of experience in Information Technology as well as those with CISA/DISA qualification, may be posted to Inspection System to the possible extent.
2. Keeping CISO: Inspection, Information Systems Audit Cell / Inspection centres Informed about various IT Polices, Procedures and guidelines, Database structure, Availability of Audit trails, Shortcomings in Application software, OS etc. by Technology Management Department.
3. Imparting periodic need based internal/external training to IS Auditors on Operating Systems, Database Management, Software Audit, Network, Audit, Penetration Testing, etc., keeping pace with the changes in IT technology and IT environment in the bank.

7.3 Periodicity of IS Audits (Schedule as per Annexure II):

7.3.1 Software Audit:

To subject all the software/patches/Hot fixes to audit by Internal Audit Team placed at ITD, before accepting any software / patches / hot fixes for implementation, so as to ensure that the software meets the procedures laid down by the bank, the following procedure shall be adopted:

- i. Infra Head to categorize the patches/hot fixes according to the urgency of release, while forwarding to Internal Audit Team, so that the audit can be completed on top priority.
- ii. CISO shall provide all necessary Inputs/infrastructure to Internal Audit Team required for the successful conduct of the audit (be it pre-Implementation or post implementation).
- iii. Any new software release/implementation status should be informed to IS Audit Cell enabling them to draw suitable IS Audit Plan for the new System.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

- iv. Emergency patches/fixes, if anything made without IS Audit, as a measure of risk mitigation due to paucity of time, the fact should be reported immediately to IS audit Cell, indicating approval of such action by the General Manager concerned.
- v. Software audit shall be carried out generally by utilizing the services of CISA/DISA qualified officers of the bank; however, the same shall be outsourced, when the software to be deployed is of highly technical in nature requiring specific skill set for such audit and such required skill set is not available Internally.

7.3.2 Network Audit:

- i. Network Audit shall conform to the broad guidelines provided under "Internet Banking Guidelines" Issued by RBI and the IT Security Policy/Procedures of the Bank.
- ii. Network audit may be initially outsourced on account of the high level of technical skill and high end tools used for penetration and other relevant tests. In course of time, CISA/DISA/CISSP qualified officers attached to core team of IS Audit shall be utilized for this task or outsourced.


7.3.3 Regular IS Audit:

7.3.3.1 Branches:

- i. IS audit of all branches shall be scheduled as per risk profile of the Branch under regular inspection and shall be carried out by the Inspecting official.
- ii. The checklist based IS Audit of Branches (Including new branches to be opened) shall be carried out along with regular Inspection of the Branch and IS audit rating arrived as per IS Audit format, shall be dovetailed to RBIA format, spelt out under Rating System (Para 8.1 of this policy).

7.3.3.2 Audit of ATMs:

1. Audit of ATMs connected to our Branches shall be carried out along with Regular Inspection of branches. This will be in addition to the review of ATM carried out by Head Office / concurrent auditors, on the following lines.
 - a) ATM audit by Inspector of Branches (including the branch under concurrent audit) and ATM audit report is followed up for rectification.
 - b) ATM Review

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

Quarterly ATM review by the concurrent auditor, in branches having concurrent auditor.

2. Inspection department to collect ATM review reports, follow up with branches for rectification of deficiencies observed and ensure that all ATMs are covered either by regular inspection or by review during that half year. The details of ATM Audit (by inspectors) & ATM review (by HO) are to be reported.

7.3.3.3 Administrative/ Other Offices where back office operations computerized:

IS Audit of PCs/Servers/Email PCs at administrative offices shall be carried out along with regular inspection of the department /office.

The following offices shall be subjected to IS Audit (Technical Audit) annually.


- i. All departments and branches.
- ii. ATM Switch / ATM Service Centre.
- iii. Data Centre, Disaster Recovery Site of CBS & ATM
- iv. NEFT/RTGS Cell etc.
- v. Rupay card Department

7.3.3.4 Other IS Audits:

The following other IS Audits have to be carried out periodically, preferably annually.

1. IS Audit of Aggregation Points (Network Equipment Routers & Switches) centrally at CISO and Centralized Data centre (CDC).
2. IS Audit of Internet Banking, Mobile banking, Tele-banking etc.,
3. IS Audit of Network infrastructure/systems with thrust on Penetration Testing
4. IS Audit covering Corporate Governance on IT Systems.
5. IS Audit of Third party IT environments, Bank shall subject IT environments of IT Service Providers to IS Audit, to verify / satisfy about the safety & security of Information Assets of the Bank in the hands of third party vendors. The Audit shall confine to the areas related to the service extended by IT Service providers to the Bank. The audit may be carried out by Banks Internal Auditors or by External Auditors, depending up on the complexity of the environment.

IS Audit Issues in Concurrent Audit: As the concurrent Audit report is submitted Quarterly, some of the critical Issues pertaining to CBS /computerized environment

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

are included in the concurrent audit checklist, to enable the concurrent auditors to point out the same so that they are addressed at the earliest.

7.4 Authorities Responsible to conduct IS Audit, Review & follow up of audit reports:

The guidelines for conducting IS Audit, authorities empowered to conduct the audit, review of the reports, issuance of closure certificates etc. are as per the IS Audit Internal guidelines document and as per the periodicity.

The IS Auditor may prepare a letter on critical matters of serious concern requiring Immediate action, if any, observed during the conduct of IS audit and submit the same directly to CIO, apart from marking a copy of the same to CISO, IS Security cell and IS Audit Cell. Special reports drawing Immediate attention may be submitted when warranted as per the guidelines spelt out in the internal guidelines.


7.5 Implementation of IS Audit Plan:

CISO is responsible for implementing and monitoring IS Audit Plans of the Bank. They are empowered to decide on the following within the overall framework of the IS Audit Policy of the Bank.

- i. IS Audit Approaches, Audit tools to be adopted within the framework of IS Security.
- ii. Policy of the bank, in co-ordination with IS Security cell.
- iii. Periodicity of IS Audits.
- iv. Bringing in of new areas/activities under the purview of IS Audit, Preparation of Checklists for conducting various IS Audits, based on guidelines / checklist issued by IS Security cell/ ITD etc. (synchronizing with RBI/ NABARD/ GOI guidelines).
- v. Issue of various guidelines with regard to carrying out of IS Audit.
- vi. Take appropriate steps to improve the quality of IS Audit in the bank.

7.6 External IS Audit Firms Engagement Letter:

These may be used for Individual assignments setting out the scope and objectives of the relationship between the external IS Audit agency and the organization. The engagement letter, namely audit charter for third party auditors should also include objectives and Information on delegation of authority to the IS Auditors. The aspects namely responsibility, authority and accountability should be considered while preparing the engagement letters.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

8. Rating of Branches under IS Audit:


Evaluation of performance and functioning of a Branch based on IS Audit findings through system of Rating is an important tool to assess vulnerability and threat associated with the IS activities of the branch. This Rating has a bearing on the performance of Branch Manager and other officials and staff. Hence, an objective system of rating is developed based on the risk associated with the various IS activities, mainly through the concept of IS audit around the computer. The Inspecting Official is required to use the same, to effectively evaluate the use of IS assets for effective performance and functioning of a branch.

8.1. Rating system under IS Audit:

- i. The following ratings will be awarded for computerized branches under IS Audit, based on their adherence to various guidelines in safeguarding the IS Assets of the bank in addition to effective and efficient use of IS Assets.
 1. Below 50% - High Risk
 2. 50 to 70% - Medium Risk
 3. Above 70% Low Risk
- ii. Inspecting official has to discuss the rating given by him with the Branch Manager concerned, on completion of IS Audit and finalization of the report. Rating given by the Inspector shall be vetted by the Inspection department and Final IS Audit Rating for the branch shall be arrived at and communicated to the Branch.
- iii. A Branch will be rated as "High Risk" either for scoring below 50 marks or for not scoring full marks under identified Compulsory Scoring Items' as indicated in the IS rating chart (due to non-adherence/non-compliance of various guidelines under IS Audit).
- iv. The above IS Audit score of the branch shall be dovetailed to RBIA rating format and IS audit report is followed up for rectification & closure along with regular RBIA.

9. Compliance:

- i. Bank's IS Audit policy generally conforms to "Information Systems Audit Policy for the Banking and Financial Sector" of Reserve Bank of India and latest RBI working group guidelines on electronic banking and Information security.

	Name of the Policy	Information system (IS) Audit Policy
	Department	Information Technology Department (ITD)
	Year	2023-24

Wherever a specific mention is not made herein, details provided in Reserve Bank of India guidelines mentioned above, shall hold good as far as it is applicable to the environment.

- ii. Inspecting officials shall ensure that the branches/offices using IT Infrastructure are strictly adhering to the various guidelines issued by CISO from time to time.
- iii. IS Audit checklists and procedures shall conform to Checklists for IS Audit provided by the Reserve Bank of India, in so far as applicable to respective IS Audit. In case of any conflict in guidelines provided therein, with the "IS Security Policy" of the bank, provisions of "IS Security Policy" will prevail over.
- iv. AGM IS Audit Cell with the approval of CISO, may devise /modify the reporting formats for Information Systems Audit, as and when required.

10. Review and Modifications to the policy:

Taking into consideration of the guidelines/circulars from RBI/NABARD, Chief Executive Officer is authorized to make suitable changes to the policy from time to time.

Sd/-
CHIEF EXECUTIVE OFFICER