The Anantapur District Cooperative Central Bank Ltd.,
Subash Road, Anantapur – 515 001 (Andhra Pradesh)
Ph.No. 274544 - Fax: (08554) 244466
Email: adccbankatp@gmail.com : ceo_atpr@apcob.org
WEB: anantapurdccb.com

Government partnered Bank

# Information Systems Audit (I S Audit) Policy 2017- 2018

## Mission Statement

***The Anantapur District Central Cooperative Bank Ltd., Anantapur is committed to achieve highest quality in IS audit in tune with the best practices in the Industry.***

### 1. Basis for I S Audit Policy

The framework and policy formulation for audit of technological risks has emanated from the report of working group constituted by RBI for finalizing the standards and procedures for ISAudit and IS security for the banking and financial sector, titled 'Information systems Audit Policy' including Information system Security guidelines and latest RBI working group guidelines on electronic banking and information security published in April 2011

### 2. Objectives & Scope of IS Audit.

### 2.1 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 Policy:**

- Safeguarding Information Systems Assets/Resources and IT Processes
- Verification of Data integrity and Security
- Evaluation of System effectiveness and efficiency:
- Verification of compliance to internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

**a) Safeguarding Information Systems Assets / Resources and IT Processes:**

a. Monitoring effective usage of Hardware, software, networking & communication facilities, people (Knowledge), system documentation, supplies etc

b. Evaluation of infrastructure (like Power, Air Conditioning, Humidity Control, physical security, Surveillance and monitoring, Incident monitoring etc ) in safeguarding of I SAssets/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.

The Anantapur District Cooperative Central Bank Ltd.,
Subash Road, Anantapur – 515 001 (Andhra Pradesh)
Ph.No. 274544 - Fax: (08554) 244466
Email: adccbankatp@gmail.com ; ceo_atpr@apcob.org
WEB: anantapurdccb.com

Government partnered Bank

# Information Systems Audit (I S Audit) Policy 2017- 2018

**Mission Statement**

***The Anantapur District Central Cooperative Bank Ltd., Anantapur is committed to achieve highest quality in IS audit in tune with the best practices in the Industry.***

## 1. Basis for I S Audit Policy

The framework and policy formulation for audit of technological risks has emanated from the report of working group constituted by RBI for finalizing the standards and procedures for ISAudit and IS security for the banking and financial sector, titled 'Information systems Audit Policy' including Information system Security guidelines and latest RBI working group guidelines on electronic banking and information security published in April 2011

## 2. Objectives & Scope of IS Audit.

### 2.1 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 Policy:**

- Safeguarding Information Systems Assets/Resources and IT Processes
- Verification of Data integrity and Security
- Evaluation of System effectiveness and efficiency:
- Verification of compliance to internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

**a) Safeguarding Information Systems Assets / Resources and IT Processes:**

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

**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, regulatoryand statutory requirements.**

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

**2.2 Scope of I S Audit:**

The scope of I S audit includes the collection and evaluation of evidence / information to determine whether the Information Systems in use safeguards the assets, maintain data security/integrity/availability, achieve the organizational goals effectively and utilize the resources efficiently. It also includes the processes for the planning and organization of theInformation Systems activity, the processes for monitoring of such activities and the examination of the adequacy of the organization and management of the I S specialist staff and non-specialists with I S responsibilities to address the I S exposures of the organization.

The I S audit covers all the computerized departments/offices of the Bank including CBS Project office / Data Centre, DR Site and branches under Core Banking Solution, Overseas Branches, Service Branches, ATM Switch and ATM service center, Credit Card Centre, Treasury Branch, NEFT/ RTGS Cell, and any other new area of IT implemented / to be implemented by the Bank. In short, it includes all the activities/areas of the organization, where IT systems are used for business purposes.

**3. I S 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 theBoard of Directors.

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 I S security policies are adhered to.

IV. Verify whether the checks and balances prescribed by I S security policy and other relevant guidelines are strictly adhered to / complied with, towards risk mitigation through proper maintenance and prevention of abuse /misuse of I T 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.

## I S Audit Setup

### 3.1 Audit Charter:

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 I S Audit.
The responsibility and accountability of internal I S auditors will be the same, as applicable togeneral inspecting officials as per the prevailing internal inspection/audit guidelines.

### 3.2 Independence:

To maintain the independence of **I S Audit function (Inspection Department**) from other departments and offices, its personnel shall report to AGM, IS AUDIT Cell. AGM, IS AUDITCell will report to Chief Audit Executive-CAE/General Manager Inspection, who shall report to the Audit Committee of the Board through Executive Director / Chairman and Managing Director.

The Inspection department shall be independent of the activities audited. The I S audit cell at CO: Inspection department and CO: I S Security Cell should be managed by two different groups to avoid conflict of interest, under different controlling authorities/ General Managers.

### 3.3 Responsibilities:

The primary responsibility of the I S Audit is to achieve the objectives of the IS Audit function as enumerated in Para 3.0 of this policy document. In brief, the responsibilities of I S Audit function of the Bank is to

I. Identify and assess potential risks to the Bank's operations.
II. Assess the means of risk mitigation and safeguarding of IT assets
III. Review the adequacy of controls established, to ensure compliance with the policies, plans, procedures, and business objectives.
IV. Assess the level of compliance to established procedures / controls
V. Assess the reliability and security of financial / management information and the systems and operations that provide this information.
VI. Assess the level of utilization of I T resources to understand their efficient and effective use for business growth.

### 3.4 Authority:

The Inspection Department / System, in the course of its I S 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 I S Audit function.

Require all members of staff and Management to supply such information and explanations asmay be needed within a reasonable period of time to I S Audit staff.

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

## 3.5 Organizational Structure

5.5.1. I S Audit resource persons of Audit Committee of the Board (ACB) - ACB will have adequately skilled composition of

- **Board of Directors**
- **Audit committee of the Board**
- **Chairman**
- **Chief Information Officer: Audit Committee**
- **I S Audit Cell**
- **Functional Heads of DCCB**
- **Functional Heads of Branches**

Directors to manage the complexity of I S Audit Oversight. A designated member of the AuditCommittee needs to possess the relevant knowledge of Information Systems, I S Controls and I S Audit issues. The designated member should also have relevant competencies 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 fillany gaps in the knowledge related to IT risks and controls.

5.5.2 - Functions of ACB on I S Audit related areas - The Audit Committee should devoteappropriate and sufficient time to I S audit findings identified during IS Audits and members ofthe Audit Committee would need to review critical issues highlighted and provide appropriateguidance to the Bank's management.

5.5.3. IS Audit Cell - Bank will have an exclusive Cell with IS Audit function, within the InspectionDepartment led by an IS Audit Head (CISO), assuming responsibility and accountability of the IS audit function, reporting tothe Chief Information Officer (CIO).

5.5.4 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.

## 5.6. Accountability

The Inspection Department shall prepare annual plan for I S 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 will prepare scoping document and Risk Based I S Audit (RBIA) Plan, covering all critical I S Assets used in CBS environment.

The plan covering I S Audit of Branches/Offices/Departments/Critical Resources approved finalized by the General Manager Inspection shall be placed for approval/adoption by ACB.

In case of need, General Manager, Inspection may make modifications to the approved plan based on the exigencies and keep ACB appraised of such modifications

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

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

I S Audit Cell shall ensure strict adherence of timely I S Audit of the I S resources as per the approved plan. The IS Audit cell (CISO: Inspection department), shall follow up the I S Audit, through Inspection centers in case of branches and through CISO, in case ofcritical resources and ensure timely rectification / compliance (by Zones for the branches andCISO for other critical resources). CISOI S Audit Cell shall place a periodic review report on the above to ACB and follow up the directions/observations of ACB are for compliance.

## 4. Administration of I S Audit

### 6.1. Conduct of Audit.

Information System Audit of branches / Offices/ Department shall be carried out as per theprescribed periodicity. I S Audit being a specialized job, the scope and function of IS Audit Cell shall be limited to organizing /conducting audit of Information and Communication Technology infrastructure used by the bank, follow up with CISO / I S Security Cell etc. for timely rectification of the deficiencies.

### 6.2. System of I S Audit:

The I S Audit Policy approved by the Board covers all the computerized Departments/Offices of the Bank including CBS Project Office / Data Centre, DR Site for CBS/ATM, Branches underCore Banking Solution, Service Branches, ATM Switch /ATM ServiceCentre, 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 I S 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 – at CISO:**

I S 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 ITassets, by way of risk mitigation for the audit of IT resources at centralized locations.

Suitable audit tools (Computer Assisted Audit Tools – CAAT) and testing accelerators for direct interrogation of the system shall be provided to the I S Auditors, in consultation/ co-ordination with CISO and Information Systems Security Cell(ISSC) for generation of certain special/specific reports. Core team of I S auditors shall be thoroughly exposed to the use of CAAT and related system tools in carrying out the I S 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. I S audit Cell at Corporate Office is established under the overall control of CO: Inspection Department for organizing and follow up of I S Audit activities of 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. The IS Audit shall be covering all the computerized departments/offices of the Bank including CBS Project Office / Data Centre, DR Site of CBS and ATM, all branches, Service Branches, ATM Switch /ATM Service centre, ATMs, Treasury Department, Debit/Credit card 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. Outsourcing may be resorted to, in areas of vital and critical importance, in case of necessary.

3. Project Office-CBS / Centralized Data Centre (PO-CBS/CDC), being the nerve centre for CBS, PO-CBS/CDC will be subjected to audit through a team of CISA qualified Auditors and report shall be submitted by them to CISO under copy to CIO shall provide all necessary inputs/infrastructure to Internal Audit Team at PO-CBS/CDC required for the successful conduct of the audit. CISO shall follow up for rectification of deficiencies and submit Action Taken Report (ATR)/ steps initiated as risk mitigation measure to I S Audit Cell within 15 days of the report.

4. Registering Authority (RA) - Digital Certificate Cell under Banking Operations Department will be subjected to half yearly internal audit and one annual external audit (using auditors empaneled by IDRBT-certifying Authority for Digital certificate) during the year and the time gap between the above two internal audits should not be more than 6 months. CISO shall follow up for rectification of deficiencies and place periodical note to CO: Audit Committee on the steps initiated /Action Taken report as risk mitigation measure

5. IS Audit Cell shall continue to function independent of IS Security Cell but work in co-ordination with them. IS Audit being a specialized job, the scope and function of IS AuditCell shall be limited to auditing of the computer based information systems and shall not include financial/transactional audit.

6. 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 I S Auditors:**

The Bank may consider engaging the services of accredited External I S Auditors/firms for I SAudit of Branches / Offices / IT infrastructure including Netware 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 I S Auditors/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.

**7.0 I S Audit Policy Guidelines:**

**7.1 General**

The checklist based I S audit shall cover all the computerized branches / departments / offices of the bank. The checklist based I S Audit of Branches (including new branches opened/ to be opened)shall be carried out along with regular inspection of the Branch (RBIA) and I S audit ratingarrived shall be dovetailed to RBIA format, as spelt out under Rating System (Para 8.1of this Policy).

**7.2 Critical Success Factors:**

The following critical factors are important for successful implementation of the I S 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 qualification, may be posted to Inspection System to the possible extent.
2. Keeping CISO: Inspection, Information Systems Audit Cell / Inspection centers informed about various IT Policies, 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 I S 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 CBSProject Office / Data Centre (PO-CBS/CDC), before accepting any software / patches / hotfixes 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 at PO-CBS/CDC, so that the audit can be completed on top priority.

II. CISO shall provide all necessary inputs/infrastructure to Internal Audit Team at POCBS/CDC 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.

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 General Manager, concerned.

V. Software audit shall be carried out generally by utilizing the services of CISA 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 qualified officers attached to core team of IS Audit shall be utilized for this task.

**7.3.3 - Regular I S Audit:**

**7.3.3.1 - Branches:**

I. I S audit of all branches shall be scheduled as per risk profile of the Branch under RBIA (regular inspection) and shall be carried out by the inspecting official conducting RBIA.

II. The checklist based I S Audit of Branches (including new branches opened/ to be opened ) shall be carried out along with regular inspection of the Branch (RBIA) and I S audit rating arrived as per IS Audit format, shall be dovetailed to RBIA format, as spelt out under RatingSystem (Para 8.1 of this policy).

**7.3.3.2 - Half yearly Computer Security Review by HO - Adherence to I S Guidelines byBranches:**

All Branches (including Service Branches) shall be subjected to half yearly Computer Security review of I S guidelines, in addition to submission of "Monthly Managers certificate on computer security", on the following lines:

I. If the branch has undergone I S Audit along with regular RBIA during that half year, it may be exempted from separate half yearly computer security review for that half year by the DCCB head Office.

II. ICs will inform Head Office, the list of branches likely to be inspected during that ensuing half year and exempt Head Office from carrying out separate half yearly computer security review for that half year covering the said branchesHO will continue with the existing system of carrying out Computer Security Review being carried out by the Branch champions/ System Managers of other branches once in a half year for all branches (except as in (i) referred above) and ensure that all the branches are subjected to half yearly computer security review either by regular inspection or by swapping System Manager of one branch to the other.

**7.3.3.3- Audit of ATMs:**

1. Audit of ATMs connected to our Branches (both on-site & Off-site ATMs) shall be carried out along with Regular inspection of branches (RBIA). This will be in addition to the review of ATM carried out by concurrent auditors, on the following lines.
   - **a) ATM audit** by inspector of Branches along with RBIA of the branch (including the branch under concurrent audit) and ATM audit report is followed up for rectification & closure along with regular RBIA.
   - **b) ATM Review**
     - i. Quarterly ATM review by the concurrent auditor, in branches having concurrent auditor
     - ii. Half yearly ATM review in other branches, by Head Office (for the half year/s, whenthere is no RBIA for that branch), through officers from nearby branches.
2. IS Audit Cell shall furnish the list of ATMs in advance to the concerned Head Offices, where such half yearly review of ATM has to be carried out.
3. IS Audit Cell to collect ATM review reports, follow up with Head Office 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/CAs) are to be reported separately in the monthly IIS report.

**7.3.3.4 Administrative/ Other Offices where back office operations are computerized:**

I S 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 I S Audit (Technical Audit) annually.**

I. DCCB branches, Treasury Department etc.
II. ATM Switch / ATM Service Centre
III. Data Centre, CBS Project Office, Disaster Recovery Site of CBS & ATM
IV. NEFT/ RTGS Cell etc
V. HRM Department
VI. Debit/Credit Card Department
VII. Registering authority (RA)- Digital certificate

**7.3.3.5 – Other I S Audits:**

**The following other I S Audits have to be carried out periodically, preferably annually.**

1. I S Audit of Aggregation Points (Network Equipment - Routers & Switches) centrally at
2. CISO and Centralized Data center (CDC).
3. I S Audit of Internet Banking, Mobile banking, Tele-banking etc.,
4. I S Audit of Network infrastructure/systems with thrust on Penetration Testing
5. I S Audit covering Corporate Governance on IT Systems.
6. I S Audit of Third party IT environments – Bank shall subject IT environments of I T
   Service Providers to I S 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.

**I S Audit Issues in Concurrent Audit:** As the concurrent Audit report is submitted monthly,some of the critical issues pertaining to CBS /computerized environment are included in theconcurrent audit checklist, to enable the concurrent auditors to point out the same so that theyare addressed at the earliest.

**7.4 Authorities Responsible to conduct I S Audit, Review & follow up of audit reports.**

The guidelines for conducting I S Audit, authorities empowered to conduct the audit, review ofthe reports, issuance of closure certificates etc are as per the I S Audit internal guidelines document and as per the periodicity detailed in the enclosed annexure- I & II.

The I S 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 theguidelines spelt out in the internal guidelines, attached with this policy as annexure-I.

### 7.5 Implementation of I S Audit Plan:

CISO is responsible for implementing and monitoring I S Audit Plans of the Bank. They are empowered to decide on the following with in the overall framework of theI S Audit Policy of the Bank.

I. I S Audit Approaches, Audit tools to be adopted within the framework of I S Security
II. Policy of the bank, in co-ordination with IS Security cell.
III. Periodicity of I S Audits.
IV. Bringing in of new areas/activities under the purview of I S Audit Preparation of Checklists for conducting various I S Audits, based on guidelines / checklist issued by IS Security cell/ ITSD/ O& M Dept etc (synchronizing with RBI/GOI guidelines).
V. Issue of various guidelines with regard to carrying out of I S Audit.
VI. Take appropriate steps to improve the quality of I S Audit in the bank.

### 7.6 External I S Audit Firms - Engagement Letter:

These may be used for individual assignments setting out the scope and objectives of the relationship between the external I S 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 following aspects, namely responsibility, authority and accountability should be considered while preparing the engagement letters.

### 8. Rating Of Branches under IS Audit:

Evaluation of performance and functioning of a Branch based on I S Audit findings through a system of Rating is an important tool to assess vulnerability and threat associated with the I S activities of the branch. This Rating has a bearing on the performance of Branch Manager andother officials and staff. Hence, an objective system of rating is developed based on the riskassociated with the various I S activities, mainly through the concept of I S audit around thecomputer. The Inspecting Official is required to use the same, to effectively evaluate the use of I Sassets 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 I S Assets of the bank in addition to effective and efficient use of I S 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 Centre and Final IS Audit Rating for the branch shall be arrived at and communicated to the Branch and Head Office.

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 I S rating chart (due to non-adherence/non-compliance of various guidelines under IS Audit).

iv. The above I S 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 I S 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 published in April 2011. 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.