

Request for Proposal for Information System (IS) Audit

**The Rajasthan State Cooperative Bank Ltd.
(RSCB)**

Request for proposal for Information System (IS) Audit

Request for Proposal for Information System (IS) Audit

RSCB/ISAUDIT/22-23/01 dated 17.5.2022

Mode of Bid Submission	Quotation based
Procuring Authority	General Manager (Administration) The RSCB Ltd., DC-1, Opposite Nehru Balodyan, Tonk Road, Jaipur (Rajasthan) – 302015
Bid Amount (Estimated Procurement Cost)	Rs.40,000 + GST per Audit
Bid Security and Mode of Payment	Bid Security – Rs.1,000/-
Bid Fee	<p>Bid Document fee is Rs.500/-</p> <p><u>The above payment of Bid Security & Bid Document fee Rs.1500/- has to be deposited through Demand Draft in favour of The Rajasthan State Co-operative Bank Ltd. payable at Jaipur or through RTGS/NEFT compulsorily. The RTGS/NEFT account details of the bank is as under:-</u></p> <p>Account Name: The Rajasthan State Co-operative Bank Ltd. Account No. : 91242100999 Branch: Head Office IFSC Code: RSCB0000001</p> <p>Scanned copy of the demand draft or RTGS/NEFT UTR receipt has to be submitted.</p>
Bid procedure	Quotation based
Bid evaluation criteria (Selection method)	Technically Qualified bidder shall be selected on Lowest Cost Based Selection (LCBS) i.e. L1 bidder
Website for downloading Bidding Document, Corrigendum's Addendums etc.	https://rscb.org.in , https://sppp.rajasthan.gov.in/ ,
Start date and time of download of Bid	17.5.2022, 10.00 AM
Last date and time of download of Bid	23.5.2022, 3.00 PM
Last Date of Submission of Bid	23.5.2022, 3.00 PM
Opening of bid	23.5.2022, 4.00 PM

Request for Proposal for Information System (IS) Audit

Bid Validity	90 days from bid submission deadline
--------------	--------------------------------------

Name of Bidding Company/ Firm:	
Contact Person (Authorized Bid Signatory):	
Correspondence Address:	
Mobile no.	
Telephone no. / Fax no.	
Website / e-mail	

**Address for Submission of Bid (Super scribe Bid Envelope with
"IS AUDIT TENDER – TO BE OPENED BY TENDER COMMITTEE ONLY")
The Rajasthan State Cooperative Bank Ltd.
DC-1, Opposite Nehru Balodyan,
Tonk Road, Jaipur-302015
Phone no. 0141-2744832, 9610780587 (System Analyst)
e-mail: rscb.ittenders@rajasthan.gov.in**

1. PROJECT PROFILE & BACKGROUND INFORMATION

The Rajasthan State Co-operative Bank Ltd., Jaipur is top tier of the three tier Short Term Co-operative Credit Structure in Rajasthan. A common data center of the RSCB & 29 DCCBs is created at the Rajasthan State Data Center, Jhalana, Jaipur. The DR Site is created at the State DR Site, Jodhpur. The branches are connected to the data center through BSNL MPLS network.

The RFP seeks to engage an Information System Auditor/ Information System Audit Firm which has capability and experience to conduct comprehensive IS Audit of Critical IT Infrastructure of RSCB and make recommendations as per the scope of work and broad guidelines for IS Audit released by the NABARD vide circular no. 33/DoS-01/2015 dated 25 February 2015 (Copy enclosed) and updated from time to time.

2. QUALIFICATION/ ELIGIBILITY CRITERIA

- A company registered under Indian Companies Act, 1956 OR A partnership firm registered under Indian Partnership Act, 1932. OR Firms registered under Limited Liability Partnership Act.
- Information System Auditor/ Information System Audit Firm should have CISA certification from ISACA, DISA (offered by ICAI), or CISSP (offered by ISC2), along with two or more years of IS Audit experience as a member
- Information System Auditor/ Information System Audit Firm should be empanelled with CERT-IN
- Information System Auditor/ Information System Audit Firm should have proven track record of conduction IS Audit as per NABARD guidelines in banks during last three years.
- Information System Auditor/ Information System Audit Firm should not have been blacklisted by any financial institution/ government departments/ other institutions. Further the name of Information System Auditor/ Information System Audit Firm should not have been in the defaulters/ barred/ caution list published at websites of the RBI, IBA, ECGC, SEBIT, CICs etc. Information System Auditor/ Information System Audit Firm should furnish self-attested affidavit on stamp paper in this regard.

3. TERMS AND CONDITIONS

1. Payment: 100% payment after completion of IS Audit and submission of IS Audit report.
2. All disputes arising out of this agreement and all questions relating to the interpretation of this agreement shall be referred to the Registrar, Co-operative Societies, Rajasthan, Jaipur for arbitration under section 58 of the Rajasthan Co-operative Societies Act, 2001.
3. All disputes are subject to Jaipur jurisdiction only.

Request for Proposal for Information System (IS) Audit

4. SCOPE OF WORK, DELIVERABLES AND TIMELINES

1. Scope of Work & Deliverables

- a. Discussion with the bank officials about the previous IS audit report observations, action taken, implementation etc.
- b. Conducting IS audit for current year and preparation of the report
- c. Verifying the action taken report on the previous audit report and observations.
- d. Verifying the new projects and Preparation of the report and discussion with the bank team.
- e. Discussion with the management on important points.
- f. Submission of IS Audit report with major observations, recommendations & CISA certification of the IS Audit.

A brief overview of the IS Audit is as under:-

Audit Domain	Audit Objective	High level Audit Scope
Data Center Audit	Review effectiveness of process, infrastructure and technology utilized for data center management	<ul style="list-style-type: none"> • Critical IT Infrastructure • Review of data Center IT infrastructure • Configuration management & Life cycle management • Capacity planning • Change management • Backup & Storage management • SLA management • Physical & logical security • Access Management • Review of controls in place • Review of asset inventory • Cyber Security management Plan (CCMP) • Security Operations Center (SOC) • Review of SOPs, AMCs, SLAs for scope, validity, adherence to standards/contracted service levels
Information System Audit	Perform Information System Audit based on requirements of bank, in view of but not limited to implementation of new application, change of application, change in	<ul style="list-style-type: none"> • Information systems Management control including application functionality, controls, reviews/ audits, • Scope comprise of the detailed guidelines released by the NABARD vide circular no. 33/DoS-01/2015 dated 25 February 2015.

Request for Proposal for Information System (IS) Audit

	hardware and network infrastructure, regulatory and statutory requirements	
IT Application Management	Review of application management activity at bank to seek assurance that appropriate controls are in place for authenticating data processing	<ul style="list-style-type: none"> • Access management/ Physical access control • Change Management/ Maintenance / change requests/ version control • Incident management including service level management • Security assessment of bank's internet, intranet sites and mobile app/ IS security policy & IS audit guidelines • Critical IT Applications • Development of software (in house/Outside)/ Application systems control • Regulatory & Software license compliance • VAPT/ Assessment against OWASP 10 vulnerabilities • Capacity planning /Operations systems control • Review of SOPs, AMCs, SLAs for scope, validity, adherence to standards/contracted service levels • Data security • Network management/Email security/ audit trails • Hardware maintenance control • Business continuation policy/Back up policy/DR/ Data warehouse. • Others: Help desk/Audit details
Independent assurance of IT Audit functions	Assess efficiency & effectiveness of IS audit for current and future business goals. Determine value addition from IS Audit to business units benchmark, identify and	<ul style="list-style-type: none"> • IS Audit scope and review • IS Audit approach • IS Audit policies review • Skill enhancement for IS Audit function for risk assessment • IS Audit roadmap

Request for Proposal for Information System (IS) Audit

	recommend successful audit practices.	
--	---------------------------------------	--

2. Duration of Audit: the audit must be completed in a week's time

3. Payment Terms

S. No.	Milestones	Payment
1	Submission of IS Audit report with major observations, recommendations & CISA certification of the IS Audit	100% payment after the submission of the report

Format for submission of Application and quotation for IS Audit work

S. No.	Items	Details	Documentary Evidence required
1.	A company registered under Indian Companies Act, 1956 OR A partnership firm registered under Indian Partnership Act, 1932. OR Firms registered under Limited Liability Partnership Act.		Certificate of Incorporation
2.	Name of Information System Auditor/ Information System Audit Firm		IS Auditor certification/ Copy of Certificate of Incorporation along with copy of latest audited balance sheet
3.	CISA certification from ISACA as a member		Copy of CISA certification
4.	CERT-IN empanelment		Copy of CERT-IN Empanelment certificate
5.	Complete Postal address		Identity & Address proof
6.	Office telephone numbers/Fax		
7.	Mobile Number		
8.	Email address		
9.	Constitution		
10.	Date of Establishment		

Request for Proposal for Information System (IS) Audit

11.	PAN of the firm/institution/Auditor (mandatory)		
12.	GST registration number (mandatory)		
13.	Location of office/branches		
14.	Name, designation, contact details of person authorized to deal with bank		
15.	Details of Information System Audits done in last 3 years	Should have name of client, list of locations, Scope of IS Audit, duration, name of reference person at client location	Copy of PO/experience certificates from respective banks
16.	Details of technical manpower for the IS Audit work (Employee name, experience, qualifications)		Copy of CISA certification
17.	Must be empanelled in latest empanelment of CERT-In		Valid CERT-IN empanelment document to be submitted by bidder
18.	Information System Auditor/ Information System Audit Firm should not have been blacklisted by any financial institution/ government departments/ other institutions.		Self-attested affidavit on stamp paper

Price Quotations

S. No.	Particulars	Cost (in Rs.) (Inclusive of GST)
1	Submission of IS Audit report with major observations, recommendations & CISA certification of the IS Audit	

Request for Proposal for Information System (IS) Audit

I/We confirm that the information furnished above is true and we have not been de-paneled / black listed by any organization in the past and we fulfill all the conditions of eligibility for Information System Audit of the Rajasthan State Co-operative Bank Ltd.

The authenticated proof in support of each of the items listed in qualifications/eligibility criteria is also enclosed.

I/We confirm that we accept and will abide by all terms and conditions of the RFP. The copy of the RFP duly signed and stamped on each page is enclosed.

Place:

Date:

Signature: (Authorized Signatory)

Designation & Address



Ref. No.NB.DoS.HO.POL/3634/J-1/2014-15

25 February 2015

[Circular No 33 / DoS-0] ./2015]

The Chairman,
All Regional Rural Banks

The Managing Director,
All State Cooperative Banks

The Managing Director/Chief Executive Officer
All Central Cooperative Banks

Madam / Dear Sir,

Introduction of Information System (IS) Audit

As you are aware, Technology Adoption by Banks and Financial Institution 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 System Audit (IS audit) in the Rural Financial Institutions like RRBs and Cooperative Banks.

2. In the wake of migration of RRBs and Cooperative Banks to Core Banking Solutions 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 us. It was observed that some of the banks had already introduced Information System Audit as a part of internal audit/inspection, while a few other banks are yet to introduce the IS audit. It has therefore, been decided to issue broad guidelines for the banks to enable them to operationalize proper IS audit mechanism.

3. Since the banking system has migrated into IT environment, it is pertinent that each bank puts in place appropriate and robust IT Policy and Information System Audit. Information system audit is the process of collecting and evaluating

evidence to determine whether the information system safeguards assets, maintains data integrity, achieves organizational goals effectively and efficiently keeping in view the IT policy of the bank. The IS audit is a planned process which is carried out on test basis. The major purpose of IS 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 types of losses and disasters, (iii) the information systems are disclosed only to those who are authorized to see and use it and not to any one 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.

4. Broad guidelines for IS Audit are indicated in Annexure-A and a check list for the guidance of Auditor carrying IS audit is furnished in Annexure-A (I) for information. While an indicative scope of IS Audit is given in Annexure – B, guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds are enumerated in Annexure B-I.

5. In the light of the above, it is advised that :

- i. The banks may adopt an IS audit policy (if not done already) appropriate to its level of computerization / CBS system adopted, with the approval of the Board and review the same at regular intervals in tune with the industry best practices and guidelines issued by RBI / NABARD from time to time.
- ii. Since most of the banks have already migrated to CBS during the recent period/ are in the process of migrating to CBS, they may, as a first step, ensure that 'Migration Audit' by a qualified firm is completed forthwith.
- iii. Banks may adopt appropriate system and practices for conducting IS audit by a qualified audit firm or by a team of competent IS personnel on annual

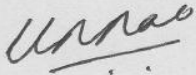
basis covering all the critically important branches (in terms of nature and volume of business) and functions at Head office / Controlling Offices.

- iv. Such audits should be preferably 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 audit reports
- v. The IS audit reports should be placed before the top management/Audit Committee of the Board / Board of Directors and the compliance should be ensured within the time frame as outlined in the audit policy.

6. This circular may be placed before the Board of Directors and Audit Committee of the Board of your bank and ensure that the guidelines are implemented with such modifications to suit local conditions and level of computerization in your bank.

7. Please acknowledge receipt of this circular to our Regional Office and confirm that the IS audit is put in place in your bank.

Yours faithfully,



(K R Rao)
Chief General Manager

Encl : as above (31 sheets)

Broad guidelines for Information System (IS) Audit

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.

1. The purpose of IS Audit is to review and provide feedback, assurance and suggestions on the concerns of the management with regard to integrity and effectiveness of systems and control. These concerns can be grouped under three areas which are related to the systems :

1.1 **Availability:** Will the information systems on which the business is heavily dependent be available for the business at all times when required ? Are the systems well protected against all types of losses and disasters? High availability systems aim to remain available at all times preventing service disruptions due to power outage, hardware failures and system upgrades.

1.2 **Confidentiality :** Will the information in the systems be disclosed only to those who is authorized to see and use it and not to anyone else ?

1.3 **Integrity :** Will the information provided by the system always be accurate, reliable and timely? What measures are available to ensure that no unauthorized modification can be made to the data or the software in the system ?

The IS audit aims to provide reasonable assurances on test basis regarding the adequacy of the controls used in the governance over IS resources and covers all the major and common types of audit, viz. Systems Audit, Application audits, Compliance audits, Security audits, Performance audits, etc.

2. Banks which have partially / fully computerized their operations and migrated on CBS system should put in place a mechanism for conducting IS audit on perpetual basis. IS audit should be conducted by a qualified auditor/ audit firm. Banks which have an independent Inspection & Audit Department should constitute an IS audit cell as part of their Inspection and Audit Department to carry out IS audit in branches / offices having computerised operations. However, those banks, which do not have an independent Inspection & Audit Department, should create a dedicated group of persons, who, when required, can perform functions of an IS Auditor. The overall control and supervision of these IS Audit Cells should be vested in the Audit Committees.

3. A team of competent and motivated IS personnel may be developed. It is beneficial to have a collective development system consisting of many persons instead of a few, in order to take care of a possible exodus of key personnel. IS auditors' technical knowledge should be augmented on a continuing basis through their deputation to seminars / conferences, supply of technical periodicals and books etc.

4. Duties of system programmer / designer should not be assigned to persons operating the system and there should be separate persons dedicated to system programming / design. System person would only make modifications / improvements to programs and the operating persons would only use such programs without having the right to make any modifications.

5. Major factors which lead to security violations in computers include inadequate or incomplete system design, programming errors, weak or inadequate logical access controls, absent or poorly designed procedural controls, ineffective employee supervision and management controls. These loopholes may be plugged by : (i) strengthening physical, logical and procedural access to system; (ii) introducing standards for quality assurance and periodically testing and checking them; and (iii) screening employees prior to induction into IS application areas and keeping a watch on their behavioral pattern.

6. There is a need for formal declaration of system development methodology, programming and documentation standards to be followed by the bank, in the absence of which quality of system maintenance / improvement might suffer. IS auditors should verify compliance in this regard.

7. Contingency plans / procedures in case of failure of system should be introduced / tested at periodic intervals. IS auditor should put such contingency plan under test during the audit for evaluating the effectiveness of such plans.

8. Every bank should have a manual of instructions for their inspectors / auditors and it should be updated periodically to keep in tune with latest developments in its area of operations and in its policies and procedures.

9. An appropriate control measure should be devised and documented to protect the computer system from attacks of unscrupulous elements. Before introducing an IS application in place of certain manual procedures, parallel run of both the systems should be done for a reasonable period to ensure that all aspects of security, reliability and accessibility of data are ensured in the IS application.

10. In order to ensure that the IS applications have resulted in a consistent and reliable system for inputting of data, processing and generation of output, various tests to identify erroneous processing, to assess the quality of data, to identify inconsistent data and to compare data with physical forms should be introduced.

11. While engaging outside computer agencies, banks should ensure to incorporate the "clause of visitorial rights" in the contract, so as to have the right to inspect the process of application and also ensure the security of the data / Data Centre / Disaster Recovery Centre / inputs given to such outside agencies. Agreement with vendor should take care of probable data leakage.

12. Entire domain of IS activities (from policy to implementation) should be brought under scrutiny of Inspection and Audit Department. Financial outlay as well as activities to be performed by IS department should be reviewed by senior management at periodic intervals.

13. The information systems auditor is to provide a report in an appropriate form, upon completion of audit work. The audit report is to state the scope, objectives, period of coverage and the nature and extent of the audit work performed. The report is to state the findings, conclusions and recommendations with respect to improvement in data integrity, system effectiveness and system efficiency.

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. Programme team and Custody of System Documentation (including programmes), confidential data, etc.?
- b. Does the Data Bank 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 exists 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 are safeguarded against unauthorized access?

II.B. Access controls: if access to programmes 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 are in vogue?
- b. Is a security package in use, or any other security facilities in O.S. and App. Packages is being explored?
- c. Is suitable security software installed and updated regularly in all systems for protecting software systems against virus, spyware, spamware and other malicious programs?
- d. Are various levels of passwords established for different transaction types, files and programmes?
- 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 that employee change the password immediately after he receives from the DBA?

II.C. Access controls: if access to programmes 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 programmes 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. programmes in use) protected from unauthorized access (i.e. use of a restricted facilities)?
- e. Is all testing activity restricted to non-production programmes and data?
- f. Do the procedures used FOR INCORPORATING NEW OR ALTERED PROGRAMMES IN PRODUCTION SYSTEMS, prevent unauthorized access to other programmes?

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 programmes?
- 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 programme execution or alteration of programme 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 programmes 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 programmes 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 programme 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. Programme approval standards?
 - ix. Implementation (including procedures for putting a programme/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 programmes?
- 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 programmes into the live environment?
- g. Do final testing procedures provide user, management, IS-staff and IS-audit personnel with a clear identification of the programme version used to perform the test?
- h. Are programmers prohibited from using live data files to test programmes?

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 programme transfer - procedures ensure that only those programmes, 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 programme changes authorized?

- a. Do policies and procedures for initiating changes to programmes and other forms of processing logic ensure that management authorizes all changes?
- b. Do policies, procedures and mechanisms ensure that personnel responsible for application programme 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 programme (s) and / or operating procedures affected by the change?

III.H. Authorization: are programme changes monitored and controlled?

- a. Do procedures ensure that all changes to the system are documented?
- b. Are programme modifications made ONLY TO COPIES OF current production programmes rather than the programmes themselves?
- c. Does a responsible official INDEPENDENT OF PROGRAMME authorize operations personnel to put a modified programme into production?
- d. Are source programmes supplied when programme 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. Programme 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. Programmes 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 programme module, subsystem?
- c. In-detail programme-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 programme listing?

- ❖ Operating System (OS) Commands listings?
- ❖ Specimen vouchers?
- ❖ Specimen data-entry (and other interface) screens?
- ❖ Specimen reports?
- ❖ Programme 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, 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?

Annex - 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)

**Guidelines on Information Security, Electronic Banking,
Technology Risk Management and Cyber Frauds**

Introduction

In the past decade, with the increased technology adoption by Banks, the complexities within the IT environment have given rise to considerable technology related risks requiring effective management.

This led the Banks to implement an Internal Control framework, based on various standards and its own control requirements and the current RBI guidelines. As a result, Bank's management and RBI, need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed.

As a consequence, the nature of the Internal Audit department has undergone a major transformation and IS audits are gaining importance as key processes are automated, or enabled by technology. Hence, there is a need for banks to re-assess the IS Audit processes and ensure that IS Audit objectives are effectively met.

The scope of IS Audit includes

- * 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
- * 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

Following areas have been covered under this chapter

- * *IS Audit* : The organisation's structure, roles and responsibilities. The chapter identifies the IS Audit stakeholders, defines their roles, responsibilities and competencies required to adequately support the IS Audit function
- * *Audit Charter or Policy (to be included in the IS Audit)* : This point addresses the need to include IS Audit as a part of the Audit Charter or Policy
- * *Planning an IS Audit* : This point addresses planning for an IS Audit, using Risk Based Audit Approach. It begins with an understanding of IT risk assessment concepts, methodology and defines the IS Audit Universe, scoping and planning an audit execution
- * *Executing an IS Audit* : This describes steps for executing the audit, covering activities such as understanding the business process and IT environment,

refining the scope and identifying internal controls, testing for control design and control objectives, appropriate audit evidence, documentation of work papers and conclusions of tests performed

- * *Reporting and Follow-up* : Describes the audit summary and memorandum, the requirements for discussing findings with the management, finalising and submitting reports, carrying out follow-up procedures, archiving documents and ensuring continuous auditing
- * *Quality Review* : This addresses the quality aspects which ensures supervision and exercising due care.

1) Role and Responsibilities / Organisational structure

Board of Directors and Senior Management

Board of Directors and senior management are responsible for ensuring that an institution's system of internal controls operates effectively. One important element of an effective internal control system is an internal audit function that includes adequate IT coverage. To meet its responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the Board, or its Audit Committee, should enable an internal audit function, capable of evaluating IT controls adequately.

Audit Committee of the Board

An institution's board of directors establishes an "Audit Committee" to oversee audit functions and to report on audit matters periodically to the Board of Directors. Banks should enable adequately skilled Audit Committee composition to manage the complexity of the IS Audit oversight.

A designated member of an Audit Committee needs to possess the knowledge of Information Systems, related controls and audit issues. Designated member should also have competencies to understand the ultimate impact of deficiencies identified in IT internal control framework by the IS Audit. The committee should devote appropriate time to IS audit findings identified during IS Audits and members of the Audit Committee need to review critical issues highlighted and provide appropriate guidance to a bank's management.

As a part of its overall responsibilities, the committee should also be ultimately responsible for the following IS Audit areas :

- * Bank's compliance with legal and regulatory requirements such as (among others) Information Technology Act-2000, Information Technology (Amendment) Act-2008, Banker's Books (Evidence) Act-1891, The Banking Regulation Act-1949, Reserve Bank of India Act-1934 and RBI circulars and guidelines
- * Appointment of the IS Audit Head
- * Performance of IS Audit
- * Evaluation of significant IS Audit issues

(A Board or its Audit Committee members should seek training to fill any gaps in the knowledge, related to IT risks and controls.)

Internal Audit / Information System Audit function

Internal Audit is a part of the Board's assurance process with regard to the integrity and effectiveness of systems and controls. It is an independent group that reports directly to the Audit Committee or the Board of Directors. IS Audit, being an integral part of Internal Audit, requires an organisation structure with well-defined roles which needs to function in alignment with the Internal Audit, and provide technical audit support on key focus areas of audit or its universe, identified by an Internal Audit department. A well-defined IS Audit organisation structure ensures that the tasks performed fulfill a bank's overall audit objective, while preserving its independence, objectivity and competence.

In this regard, banks require a separate IS Audit function within an Internal Audit department led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE). The personnel needs to assume overall responsibility and accountability of IS Audit functions. Where the bank leverages external resources for conducting IS Audit on areas where skills are lacking, the responsibility and accountability for such external IS Audits still remain with the IS Audit Head and CAE.

Critical Components and Processes

- (i) Because the IS Audit is an integral part of the Internal Auditors, 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. 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.

Additionally, to ensure independence for the IS Auditors, Banks should make sure that :

- * Auditors have access to information and applications
- * Auditors have the right to conduct independent data inspection and

analysis

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 a bank. They should be competent audit professionals with sufficient and relevant experience. Qualifications such as CISA (offered by ISACA), DISA (offered by ICAI), or CISSP (offered by ISC2), 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.

(ii) Outsourcing relating to IS Audit

Banks 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 the CAE and the Audit Committee. This may be due to inadequate staff available internally within the bank to conduct audits, or insufficient levels of skilled staff. The work outsourced shall be restricted to execution of audits identified in the plan. Banks need to ensure that the overall ownership and responsibility of the IS Audit, including the audit planning process, risk assessment and follow-up of compliance remains within the bank. External assistance may be obtained initially to put in place necessary processes in this regard.

Both the CAE 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.

2) Audit Charter, Audit Policy to include IS Audit

Audit Charter or Policy is a document, which guides and directs activities of an internal audit function. IS Audit, being integral part of an Internal Audit department, should also be governed by the same charter or policy. The charter should be documented to contain a clear description of its mandate, purpose, responsibility, authority and accountability of relevant members or officials in respect of the IS Audit (namely the IS Auditors, management and Audit Committee) apart from the operating principles. 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 any departure there from.

(a) **Contents of the Audit Policy**

The Policy should clearly address the aspects of responsibility, authority and accountability of the IS auditor. Aspects to be considered :

Responsibility :

Some of the aspects include :

1. Mission Statement
2. Scope or Coverage
3. Audit Methodology
4. Objectives
5. Independence
6. Relationship with External Audit
7. Auditee's Requirements
8. Critical Success Factors
9. Key Performance Indicators
10. Other Measures of Performance
11. Providing Assurance on Control Environment
12. Reviewing Controls on Confidentiality, Integrity and Availability of Data or Systems

Authority :

Includes the following :

1. Risk Assessment
2. Mandate to perform an IS Audit
3. Allocation of resources
4. Right to access the relevant information, personnel, locations and systems
5. Scope or limitations of scope
6. Functions to be audited
7. Auditee's expectations
8. Organizational structure
9. Gradation of IS Audit Officials or Staff

Accountability : Some of the aspects in this regard include the following :

1. Reporting Lines to Senior Management, Board of Directors or Designated Authority
2. Assignment Performance Appraisals
3. Personnel Performance Appraisals
4. Staffing or Career Development
5. Training and Development of Skills including maintenance of professional certification/s, continuing professional education
6. Auditees' Rights
7. Independent Quality Reviews
8. Assessment of Compliance with Standards
9. Benchmarking Performance and Functions
10. Assessment of Completion of the Audit Plan
11. Agreed Actions (e.g. penalties when either party fails to carry out responsibilities)
12. 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 should also be annual review of IS Audit Policy or Charter to ensure continued relevance.

(b) Communication with the Auditees

Effective communication with the auditees involves considering the following:

- * Describing a service, its scope, availability and timeliness of delivery
- * Providing cost estimates or budgets, if needed
- * Describing problems and possible resolutions
- * Providing adequate and accessible facilities for effective communication
- * Determining 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

(c) **Quality Assurance Process**

The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, or assignment performance surveys) to understand his expectations relevant to the function. These needs should be evaluated against the Charter, to improve the service or change the service delivery or Audit Charter, if necessary.

(d) **Engagement Letter**

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

Following aspects needs to be considered :

Responsibility: The aspects addressed includes scope, objectives, independence, risk assessment, specific auditee requirements and deliverables

Authority : The aspects to be addressed include right of access to information, personnel, locations and systems relevant to the performance of the assignment, scope or any limitations of scope and documentary evidence or information of agreement to the terms and conditions of the engagement

Accountability : Areas addressed include designated or intended recipients of reports, auditees' rights, quality reviews, agreed completion dates and agreed budgets or fees if available

3) Planning an IS Audit

(a) **Introduction**

An effective IS Audit programme 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 programme is essential to evaluate risk management practices, internal control systems and compliance with policies concerning IT related risks of every size and complexity. Effective programmes 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 Characterisation
- * **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
- * **Scoping for IS Audit** : This addresses the scoping 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 :

(b) **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". Principles in the guidance note may be made use of by RRBs and Cooperative Banks.

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 programme scope and resource allocation for each area audited
- Implementation of the Audit Plan

(c) 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.

A successful risk-based IS Audit Programme can be based on an effective scoring system arrived at by considering all relevant risk factors.

Major risk factors used in scoring systems include : Adequacy of internal controls, business criticality, regulatory requirements, amount or value of transactions processed, if a key customer information is held, customer facing systems, financial loss potential, number of transactions processed, availability requirements, experience of management and staff, turnover, technical competence, degree of delegation, technical and process complexity, stability of application, age of system, training of users, number of interfaces, availability of documentation, extent of dependence on the IT system, confidentiality requirements, major changes carried out, previous audit observations and senior management oversight.

On the basis of risk matrix of business criticality and system or residual risk, applications or systems can be graded, based on where they fall on the "risk map" and accordingly their audit frequency can be decided. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these with the Audit Committee or the Board. Risk assessment guidelines will vary for banks depending on size, complexity, scope of activities, geographic diversity and technology systems used. Auditors should use the guidelines to grade major risk areas and define range of scores or assessments (e.g., groupings such as low, medium, or high risk or a numerical sequence such as 1 to 5).

The written risk assessment guidelines should specify the following elements :

- * **Maximum length for audit cycles based on the risk assessment process :** For example, very high to high risk applications audit cycle can be at a frequency ranging from six months upto 12, medium risk applications can be 18 months (or below) and up to 36 months for low-risk areas. Audit cycles should not be open-ended.
- * **Timing of risk assessments for each business area or department :** While risk assessment is expected to be on an annual basis, frequent assessments may be needed if an institution experiences rapid growth or change in operation or activities.
- * **Documentation requirements to support risk assessment and scoring decisions**
- * **Guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden :** Example : due to major changes in system, additional regulatory or legal requirements, a medium risk application may have to be audited more frequently.

Notwithstanding the above, IT governance, information security

governance-related aspects, critical IT general controls such as data centre controls and processes and critical business applications / systems having financial / compliance implications, including regulatory reporting, risk management, customer access (delivery channels) and MIS systems, needs to be subjected to IS Audit at least once a year (or more frequently, if warranted by the risk assessment).

IS Auditors should periodically review results of internal control processes and analyse financial or operational data for any impact on a risk assessment or scoring. Accordingly, auditee units should be required to keep auditors up-to-date on major changes, such as introduction of a new product, implementation of a new system, application conversions, significant changes in organisation or staff, regulatory and legal requirements, security incidents.

(d) **Defining the IS Audit Universe**

An Audit Universe is an outcome of the risk assessment process. It defines the audit areas to be covered by the IS Auditor. It is usually a high-level structure that identifies processes, resources, risks and controls related to IT, allowing for a risk-based selection of the audit areas. The IT risks faced by banks due to emerging technologies, prioritisation of IS Audit Universe, selection of types of audits that need to be performed, optimisation of available resources, and ensuring quality of findings, are challenges faced by IS Audit.

The IS Audit Universe can be built around the four types of IT resources and processes : Such as application systems, information or data, infrastructure (technology and facilities such as hardware, operating systems, database management systems, networking, multimedia, and the environment that houses and supports them and enable processing of applications) and people (internal or outsourced personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services).

The challenge is to provide the "right level of granularity" in the definition of the universe, so as to make it effective and efficient.

Though this is different for every bank, below are some of the considerations for defining IS Audits :

- * **Using overly-broad definitions for IS Audits (e.g. IT general controls) will ensure a scope creep in audit procedures.** The IS Audit Head should make sure that the definition of each IS Audit is an accurate description of what is being reviewed.
- * **Audit Universe for a year should touch upon all layers in the IT environment.** Though each IT environment is different, layers tend to be the same. If an IS Audit plan does not include some review for

each of the layers, odds are that the plan, as a whole, is deficient.

* **IS Audits should be structured in such a way as to provide for effective and logical reporting.** For example : IS Audits of pervasive technologies (e.g. networks or processes) are more effective when audited at an enterprise level.

* **IS Audits should address appropriate risks.** In many cases, IS Audit budgets are determined before the IT risk assessment is performed. This inevitably leads to one of two situations :

An inadequate number of audit hours are spread over too many audits, which results in consistently poor quality audits, because there is not enough time.

Audits that should be performed are not performed because the budget does not allow it.

(e) **Scoping for IS Audit**

Information gathered by the IS Auditors during IT risk assessment about the IT system processing and operational environment, threats, vulnerabilities, impact and controls, enables identification of the control objectives and activities to be tested for design and implementation effectiveness and its operating effectiveness.

Scoping plays a crucial role in overall effectiveness. This is exacerbated by the need for the IS Auditors to integrate with the process, operational or financial auditors, and the procedures they are performing, particularly in environments with large integrated CBS applications, where a high number of key process controls are contained within the systems.

IS Audits should also cover branches, with focus on large and medium branches, in areas such as control of passwords, user ids, operating system security, anti-malware, maker-checker, segregation of duties, physical security, review of exception reports or audit trails, BCP policy and or testing.

Reports and circulars issued by RBI / NABARD for specific areas which also need to be covered in the IS Audit Scope :

(i) Defining Control Objectives and Activities

IT control objectives, based on well known frameworks can be included in the scope.

(ii) Materiality

When conducting financial statement audits, Internal Auditors measure materiality in monetary terms, since areas that are audited

are also measured and reported in monetary terms. However, since IS Auditors conduct audit on non-financial items, alternative measures are required to assess materiality. Such assessments are a matter of professional judgment. They include consideration of its effect on a bank as a whole, of errors, omissions, irregularities and illegal acts, which may have happened as a result of "internal control weaknesses" in an area being audited. ISACA IS Auditing Guideline G6 : specifies that if the IS Audit focus relates to systems or operations that process financial transactions, the value of assets controlled by the system(s), or the value of transactions processed per day / week / month / year, should be considered in assessing materiality. In case, the focus is on systems that do not process financial transactions, then following measures should be considered :

- * Criticality of the business processes supported by the system or operation
- * Cost of system or operation (hardware, software, staff, third-party services, overheads or a combination of these)
- * Potential cost of errors (possibly in terms of irrecoverable development costs, cost of publicity required for warnings, rectification costs, health and safety costs, high wastage, etc.)
- * Number of accesses / transactions / inquiries processed per period
- * Nature, timing and extent of reports prepared, and files maintained
- * Service-level agreement requirements and cost of potential penalties
- * Penalties for failure to comply with legal and contractual requirements

IS Auditors should review the following additional areas that are critical and high risk such as :

- IT Governance and information security governance structures and practices implemented by the Bank
- Testing the controls on new development systems before implementing them in live environment.
- A pre-implementation review of application controls, including security features and controls over change management process, should be performed to confirm that :
 - * Controls in existing application are not diluted, while migrating data to the new application

- * Controls are designed and implemented to meet requirements of a bank's policies and procedures, apart from regulatory and legal requirements
- * Functionality offered by the application is used to meet appropriate control objectives
- A post implementation review of application controls should be carried out to confirm if the controls as designed are implemented, and are operating, effectively. Periodic review of application controls should be a part of an IS audit scope, in order to detect the impact of application changes on controls. This should be coupled with review of underlying environment-operating system, database, middleware, etc.-as weaknesses in the underlying environment can negate the effectiveness of controls at the application layer. Due care should be taken to ensure that IS Auditors have access only to the test environment for performing the procedures and data used for testing should be, as far as practical, be a replica of live environment.
- Detailed audit of SDLC process to confirm that security features are incorporated into a new system, or while modifying an existing system, should be carried out.
- A review of processes followed by an implementation team to ensure data integrity after implementation of a new application or system, and a review of data migration from legacy systems to the new system where applicable, should be followed.
- IS Auditors may validate IT risks (identified by business teams) before launching a product or service. Review by IS Auditor may enable the business teams to incorporate additional controls, if required, in the system before the launch.

(iii) Building Fraud Risk Perspective

In planning and performing an audit to reduce risks to a low level, the auditor should consider the risk of irregularities and illegal acts. He should maintain professional scepticism during an audit, recognising the possibility that "material mis-statements due to irregularities and illegal acts" could exist, irrespective of their evaluation of risk of irregularities and illegal acts.

IS Auditors are also required to consider and assess the risk of fraud, while performing an audit. They should design appropriate plans, procedures and tests, to detect irregularities, which can have a material effect on either a specific area under an audit, or the bank as a whole. IS Auditors should consider whether internal control weaknesses could result in material irregularities, not being prevented or detected. The auditor should design and perform procedures to test the appropriateness of internal control and risk of

override of controls. They should be reasonably conversant with fraud risk factors and indicators, and assess the risk of irregularities connected with the area under audit.

In pursuance to the understanding gathered during threat identification step of the IT Risk Assessment process, the auditors should identify control objectives and activities. These are required to be tested to address fraud risk. He should consider "fraud vulnerability assessments" undertaken by the "Fraud Risk Management Group", while identifying fraud risk factors in the IT risk assessment process. He should be aware that certain situations may increase a bank's vulnerability to fraud risk (e.g. introduction of a new line of business, new products, new delivery channels and new applications or systems.)

In preparing an audit scope, auditors should consider fraud risk factors including these :

1. Irregularities and illegal acts that are common to banking industry
2. Corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of performance pressures
3. Management's behaviour with regard to ethics
4. Employee dissatisfaction resulting from potential layoffs, outsourcing, divestiture or restructuring
5. Poor financial or operational performance
6. Risk arising out of introduction of new products and processes
7. Bank's history of fraud
8. Recent changes in management teams, operations or IT systems
9. Existence of assets held, or services offered, and their susceptibility to irregularities
10. Strength of relevant controls implemented
11. Applicable regulatory or legal requirements
12. History of findings from previous audits
13. Findings of reviews, carried out outside the audit, such as the findings from external auditors, consultants, quality assurance teams, or specific investigations
14. Findings reported by management, which have arisen during the day-to-day course of business
15. Technical sophistication and complexity of the information system(s)

supporting the area under audit

16. Existence of in-house (developed or maintained) application systems, as compared with the packaged software for core business systems

Instances of fraud should be reported to appropriate authority including CFMC, DoS, NABARD, HO :

NABARD (vide its circular NB. DoS. HO. POL. CFMC . No. 62 / DoS -03 /2014, dated: April 17, 2014) requires that fraud cases should be reported to the NABARD. Banks should appropriately include requirements for reporting to NABARD, of such instances, in engagement letters issued to external IS Auditors.

(f) Planning the Execution

The IS Audit Head is responsible for the annual IS Audit Plan, prepared after considering the risk assessment and scoping document. The plan covers overall audit strategy, scoped areas, details of control objectives identified in the scoping stage, sample sizes, frequency or timing of an audit based on risk assessment, nature and extent of audit and IT resource skills availability, deployment and need for any external expertise. A report on the status of planned versus actual audits, and any changes to the annual audit plan, needs to be periodically presented to Audit Committee and Senior Management on a periodic basis. There are well-known guidance on IS Audit. The Institute of Chartered Accountants of India (ICAI), in March 2009, published the "Standard on Internal Audit (SIA) 14 : Internal Audit in an Information Technology Environment" covering requirements of the planning stage, which an auditor should follow. IIA has provided guidance on defining the IS Audit Universe, through the guide issued on "Management of IS Auditing" under the "Global Technology Audit Guide" series. ITGI has provided guidance on audit planning in its "IT Assurance Guide using COBIT".

Suggested guidelines for implementation by banks are as follows :

i. Documenting the Audit Plan

The plan (either separately or as part of overall internal audit plan) should be a formal document, approved by the Audit Committee initially and during any subsequent major changes. The plan should be prepared so that it is in compliance with any appropriate external requirements in addition to well-known IS Auditing Standards.

Audit Plan Components include :

- * **Internal Audit Subject** : Name of the Audit Subject
- * **Nature of Audit** : Compliance with legal, regulatory or standards, performance metrics assessment or security configuration testing
- * **Schedule** : Period of audit and its expected duration

- * **Scoped Systems** : Identified IT resources that are in the scope based on the risk assessment process
- * **System Overview** : Details of System Environment based on the risk assessment process
- * **Audit Details** : Details of risks and controls identified, based on the risk assessment process
- * **Nature and Extent of Tests** : Controls testing for effectiveness of design and implementation of controls, substantive testing for operating effectiveness of controls implemented
- * **Method of Internal Audit** : Brief audit approach and methodology
- * **Team and Roles and Responsibilities** : Identified skills and names of IS Auditors including their roles and responsibilities
- * **Points of Contact** : Contact names of auditee department
- * **Co-ordination** : Names of the project lead and higher official for escalation of issues
- * **Information** : Report details of past audits on the subject

ii. **Nature and Extent of Tests of Control**

Types of testing that can be performed are as below :

- * **Test of Control Design** : Controls that have been identified are evaluated for appropriateness in mitigating the risks
- * **Test of Control Implementation** : Tests are performed to confirm that the control that has been appropriately designed is implemented and is operating at the time of testing. Mitigating or compensating controls are also reviewed wherever necessary
- * **Assessing Operational Effectiveness of Controls** : Wherever the controls designed are found to be in operation, additional testing is performed for the period of reliance (audit period) to confirm if they are operating effectively and consistently On case-to-case basis, the auditor should exercise professional judgment and decide the nature and extent of procedures that need to be adopted for conclusions. ISA 330 gives guidance on the nature, timing and extent of procedures.

iii. **Sampling techniques**

During an audit, auditors should obtain sufficient, reliable and relevant evidence to achieve their objectives. Findings and conclusions should be supported by appropriate analysis and interpretation. Auditors should consider sample selection techniques, which result in a statistically-based representative sample for

performing compliance or substantive testing. Statistical sampling involves the use of techniques from which mathematically-constructed conclusions regarding the population can be drawn. Non-statistical sampling is not statistically-based. Its results should not be extrapolated over the population as a sample is unlikely to be representative of the population. Examples of compliance testing of controls where sampling could be considered, include user-access rights, programme change control procedures, procedures documentation, programme documentation, follow-up of exceptions, review of logs and software licences audits. Examples of substantive tests where sampling could be considered, include re-performance of a complex calculation (e.g., interest applied), on a sample of accounts, sample of transactions to vouch to supporting documentation, etc.

Design of A Sample

While designing the size and structure of an audit sample, auditors may consider the following guidelines :

- **Sampling Unit** : The unit will depend on the sample purpose. For compliance testing of controls, attribute sampling is typically used, where the unit is an event or transaction (e.g., a control such as an authorisation of transaction).
- **Audit objectives** : IS Auditors should consider the audit objectives to be achieved and the audit procedures, which are most likely to achieve those objectives. In addition, when sampling is appropriate, consideration should be given to the nature of the audit evidence sought, and possible error conditions.
- **Population** : Population is an entire set of data from which auditors wish to sample, in order to reach a conclusion. Hence, the population from which a sample is drawn, has to be appropriate and verified as a "complete" for audit objective.
- **Stratification** : To assist in efficient and effective design of a sample, stratification may be appropriate. Stratification is a process of dividing a population into "sub-populations" with similar characteristics, explicitly defined, so that each sample unit can belong to only one stratum.

Selection of A Sample

IS Auditors should use statistical sampling methods. They may consider using the following :

- **Random Sampling** : It ensures that all combinations of units in the population have an equal chance of selection
- **Systematic Sampling** : It involves selecting units using a fixed

interval between selections, the first interval having a random start. Examples include "Monetary Unit Sampling" or "Value Weighted Selection", where each individual monetary value (e.g., Rs.100) in the population, is given an equal chance of selection. As an individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts, but gives every monetary value an equal opportunity for selection. Another example includes selecting every 'nth sampling unit'.

iv **Standards and Frameworks**

One challenge that the IS Auditors face is knowing what to audit against as a fully-developed IT control baselines for applications and technologies that may not have been developed. Rapid evolution of technology is likely to render baselines useless, after a period of time. However, this does not detract from the concept of control objectives.

Control objectives, by definition, should remain more or less constant (from environment to environment). Consider the objective that critical business data and programmes should be backed up and recoverable. Now, each environment may do that differently; backups could be manual, or automated, or a tool may be used. They could be incremental only, or there may be complete backups of everything. Backups could be done daily, weekly, or monthly. Storage of backups could be onsite in a fireproof safe, off-site at another company facility, or outsourced to a third party. Method used by the organisation to manage backups would certainly impact the audit procedures and budget, but the control objective will not change. IS Auditor should be able to start with a set of IT control objectives, and though not specific to particular environments, select an appropriate framework.

v. **Resource Management**

A bank's auditors play a critical role in efficiency and effectiveness of audits. IT encompasses a wide range of technology and sophistication-the skill set needed to audit a Firewall configuration is vastly different from the skill set needed to audit application controls. It is critical to match the skills needed to perform a particular IS Audit, with the appropriate auditor. IS Auditors should also have the appropriate analytical skills to determine and report the root cause of deficiencies. Bank's hiring and training practices should ensure that it has qualified IS Auditors where education and experience should be consistent with job responsibilities. Audit management should also

provide an effective programme of continuing education and development.

The main issue is having staff with the requisite range of IS Audit skills, needed to audit an IS Audit universe, effectively. If internal expertise is inadequate, the Board should consider using qualified external sources, such as management consultants, independent auditors, or professionals, to supplement internal resources and support bank's objectives.

4) Executing IS Audit

As mentioned earlier, auditors must understand the business and IT environment, risks and internal control framework. During audit, auditors should obtain evidences, perform test procedures, appropriately document findings, and conclude a report. This section provides guidance on matters that IS Auditor should consider while executing the Plan.

ICAI, in March 2009, had published a "Standard on Internal Audit (SIA) 14: Internal Audit in an Information Technology Environment" covering the requirements of executing a plan that an IS Auditor should follow. Additionally, IIA has also provided guidance in their "Management of IS Auditing" under their "Global Technology Audit Guide" series. The ITGI has also provided guidance on execution of assurance initiative in its "IT Assurance Guide Using COBIT".

Guidance on executing the IS Audit entails the following steps :

- Refining the understanding of business process and IT environment
- Refining the scope and identifying internal controls
- Testing Control Design
- Testing the outcome of the control objectives
- Collecting audit evidence
- Documenting test results
- Concluding tests performed
- Considering use of audit accelerators
- Considering the use of Computer-Aided Automated Tools (CAATs)
- Considering the work of others
- Considering third-party review by service providers

The above are covered in the following sections :

(a) Refine understanding of the business process and IT environment :

The first step of the execution stage is refining the understanding of an IT environment, in which a review is being planned. This implies understanding

of a bank's business processes to confirm the correct scope and control objectives. The scope of the IS Audit need to be communicated to and agreed upon by stakeholders.

Output from this step consists of documented evidence regarding :

- Who performs the task(s), where it is performed and when
- Inputs required to perform the task and outputs generated by it
- Automated tasks performed by systems and system configurations
- System-generated information used by business
- Stated procedures for performing tasks

The IS Auditor can structure this step along the following lines :

- Interview and use activity lists and RACI charts
- Collect and read process description, policies, input or output, issues, meeting minutes, past audit reports, past audit recommendations, business reports
- Prepare a scoping task (process objective, goals and metrics)
- Build an understanding of enterprise IT architecture

(b) Refining Scope and Identifying Internal Controls

While understanding and evaluating internal controls of a bank, areas mentioned under "Scope of IS Audit" needs to be covered. However, the nature and extent of control risks may vary, depending on nature and characteristics of a bank's information system :

- Reliance on systems or programmes that are inaccurately processing data, or processing inaccurate data, or both
- Unauthorised access to data which may result in destruction of data, or improper changes to data, including recording of unauthorised or non-existent transactions, or inaccurate recording of transactions
- Possibility of IT personnel gaining access to privileges, beyond those necessary, to perform their assigned duties, thereby breaking down segregation of duties
- Unauthorised changes to data in master files
- Unauthorised changes to systems or programmes

Failure to make necessary changes to systems or programmes

- Inappropriate manual intervention
- Potential loss of data or inability to access data

(c) Testing Control Design

This section lists the different techniques that will be used in detailed audit steps. Testing of controls is performed covering the main test objectives :

- Evaluation of control design
- Confirmation that controls are in place within the operation
- Assess the operational effectiveness of controls
- Additionally, control efficiency could be tested

In the testing phase, different types of testing can be applied. Five generic testing methods include enquire and confirm, inspect, compare actual with expected findings, re-perform or re-calculate and review automated evidence collection through analyzing data using computer assisted audit techniques and extracting exceptions or key transactions.

To assess the adequacy of the design of controls the following steps should be performed :

- Observe, inspect and review control approach. Test the design for completeness, relevance, timeliness and measurability
- Enquire whether, or confirm that, the responsibilities for control practices and overall accountability have been assigned
- Test whether accountability and responsibilities are understood and accepted. Verify that the right skills and the necessary resources are available
- Enquire through interviews with key staff involved whether they understand the control mechanism, its purpose and the accountability and responsibilities.

IS Auditor must determine whether :

- Documented control processes exist
- Appropriate evidence of control processes exists
- Responsibility and accountability are clear and effective
- Compensating controls exist, where necessary

Additionally, specifically in internal audit assignments, cost-effectiveness of a control design may also be verified, with the following audit steps :

- **If the control design is effective :** Investigate whether it can be made more efficient by optimising steps, looking for synergies with other mechanisms, and reconsidering the balance of prevention versus detection and correction. Consider the effort spent in maintaining the control practices
- **If the control is operating effectively :** Investigate whether it can

be made more cost effective. Consider analysing performance metrics of activities associated, automation opportunities or skill level

(d) **Test the Outcome of Control Objectives**

Audit steps performed ensure that control measures established are working as prescribed and conclude on the appropriateness of the control environment. To test the effectiveness of a control, the auditor needs to look for direct and indirect evidence of the control's impact on the process outputs. This implies the direct and indirect substantiation of measurable contribution of the control to the IT, process and activity goals, thereby recording direct and indirect evidence of actually achieving the outcomes or various control objectives (based on those documented in standards like COBIT, as relevant).

The auditor should obtain direct or indirect evidence for selected items or periods to ensure that the control under review is working effectively by applying a selection of testing techniques as presented in step on test of control design. The IS Auditor should also perform a limited review of the adequacy of the process deliverables, determine the level of substantive testing and additional work needed to provide assurance that the IT process is adequate. Substantive testing would involve performing analytical procedures and tests of details, to gain assurance on areas where control weaknesses are observed. Substantive testing is performed to ascertain the actual impact of control weaknesses.

(e) **Audit Evidence**

IS Auditors should obtain sufficient and reliable audit evidence to draw reasonable conclusions on which to base the audit results.

Sufficient Evidence : Evidence can be considered sufficient if it supports all material questions in the audit objective and scope. Evidence should be objective and sufficient to enable a qualified independent party to re-perform tests and obtain the same results. The evidence should be commensurate with the materiality of an item and risks involved. In instances where IS Auditor believes sufficient audit evidence cannot be obtained, they should disclose this in a manner consistent with the communication of the audit results.

Appropriate Evidence : Appropriate evidence shall include the following indicative criteria :

- Procedures as performed by the IS Auditor
- Results of procedures performed by the IS Auditor
- Source documents (electronic or paper), records and corroborating information used to support the audit
- Findings and results of an audit

When obtaining evidence from a test of control design, auditors should consider the completeness of an audit evidence to support the assessed level of control risk.

Reliable Evidence : IS Auditors should take note of following examples of evidence that is more reliable when it is :

- Written form and not oral expressions
- Obtained from independent sources
- Obtained by IS Auditors, rather than from the bank being audited
- Certified by an independent party

Procedures used to gather evidence can be applied through the use of manual audit procedures, computer-assisted techniques, or a combination of both. For example: a system, which uses manual control totals to balance data entry operations might provide audit evidence that the control procedure is in place by way of an appropriately reconciled and annotated report. IS Auditors should obtain audit evidence by reviewing and testing this report. Detailed transaction records may only be available in machine-readable format, requiring IS Auditors to obtain evidence using computer-assisted techniques.

When information produced by a bank is used by auditors, they should obtain evidence about the completeness and accuracy by the following means :

- Performing tests of the operating effectiveness of controls over the production and maintenance of information, to be used as audit evidence
- Performing audit procedures directly on information to be used as audit evidence

Auditors should consider the following controls over production and maintenance of information produced by a bank :

- Controls over the integrity, accuracy, and completeness of the source data
- Controls over the creation and modification of the applicable report logic and parameters

(f) **Documentation**

Audit evidence gathered should be documented and organised to support findings and conclusions. IS Audit documentation is a record of the work performed and evidence supporting findings and conclusions.

The potential uses of documentation

- Demonstration of the extent to which the auditor has complied with professional standards related to IS auditing
- Assistance with audit planning, performance and review
- Facilitation of third-party reviews
- Evaluation of the auditors' quality assurance programme
- Support in circumstances such as insurance claims, fraud cases and lawsuits
- Assistance with professional development of the staff

Documentation should include, at a minimum, a record of

- Planning and preparation of the audit scope and objectives
- Audit steps performed and audit evidence gathered
- Audit findings, conclusions and recommendations
- Reports issued as a result of the audit work
- Supervisory review

Extent of an IS Auditor's documentation may depend on needs for a particular audit and should include such things as :

- IS Auditor's understanding of an area to be audited, and its environment
- His understanding of the information processing systems and internal control environment
- Audit evidence, source of audit documentation and date of completion
- Bank's response to recommendations

Documentation should include audit information, required by law, government regulations, or by applicable professional standards. Documentation should be clear, complete and understandable, by a reviewer. IS Audit owns evidences documented by them, in order to substantiate conclusions on tests performed and specific observations reported to management and Audit Committee.

(g) Conclusion on Tests Performed

IS Auditors should evaluate conclusions drawn as a basis for forming an opinion on the audit. Conclusions should be substantiated by evidences, collected and documented. The IS Audit Team may be required to provide and maintain evidences in respect of observations reported by them.

IS Auditors may perform following activities required to conclude on tests performed based on nature and amount of identified control failures and

likelihood of undetected errors:

- Decide whether the scope of IS Audit was sufficient to enable the auditors to draw reasonable conclusions on which to base audit opinion
- Perform audit procedures designed to obtain sufficient appropriate audit evidence: events upto the date of audit report may be included and identified in the report
- Prepare an audit summary memorandum documenting findings and conclusions on important issues of IS Auditing and reporting, including judgments made by an IS Audit team
- Obtain appropriate representations from bank management
- Prepare a report appropriate to circumstances, and in conformity with, applicable professional standards and regulatory and legal requirements
- Communicate, as necessary, with Audit Committee or Senior Management
- Maintain effective controls over processing and distribution of reports relating to the IS Audit

If audit evidence or information indicate that irregularities could have occurred, IS auditors should recommend the bank management on matters that require detailed investigation to enable the management to initiate appropriate investigative actions. The auditors should also consider consulting the Audit Committee and legal counsel about the advisability and risks of reporting the findings outside the Bank.

(h) **Audit Accelerators**

Since IS Audit budgets can be difficult to estimate and manage, CAEs can consider using testing accelerators-tools or techniques that help support procedures that the IS Auditors will be performing -to increase efficiency and effectiveness. CAEs can use an accelerator to do the same audit in less time, or do more detailed audit procedures in the same amount of time. Audit accelerators can be divided into two categories:

- **Audit Facilitators** : Tools that help support the overall management of an audit (e.g., an electronic workpaper management tool)
- **Testing Accelerators** : Tools that automate the performance of audit tests (e.g., data analysis tools).

Audit Facilitators

These include Electronic Work papers, project management software, flow charting software and open issue tracking software.

Testing Accelerators

Testing accelerators can automate time-consuming audit tasks, such as reviewing large populations of data. Also, using a tool to perform audit procedures helps establish consistency. For example, if a tool is used to assess server security configuration, servers tested with that tool will be assessed along the same baselines. Performing these procedures manually allows for a degree of interpretation on the part of the IS Auditor. Lastly, the use of tools enables IS Auditors to test an entire population of data, rather than just a sample of transactions. This provides for a much higher degree of audit assurance.

Data Analysis Software : These allow an auditor to perform robust statistical analysis of large data sets. They can also be used to support process or operational audits like KYC reviews. They can support types of testing. One consideration when using a data analysis tool is that it may be difficult to extract the data from the original source. It is critical that audit procedures be performed to ensure the completeness and accuracy of the source data.

Security Analysis Tools : These are a broad set of tools that can review a large population of devices or users and identify security exposures. There are different types of security analysis tools. Generally they can be categorised as follows :

- Network Analysis Tools: These consist of software programmes that can be run on a network and gather information about it. IS Auditors can use these tools for a variety of audit procedures, including :

Verifying the accuracy of network diagrams by mapping corporate network
Identifying key network devices that may warrant additional audit attention
Gathering information about what traffic is permitted across a network (which would directly support the IT risk assessment process).

- Hacking Tools: Most technologies have a number of standard vulnerabilities, such as the existence of default IDs and passwords or default settings when the technology is installed out-of-the-box. Hacking tools provide for an automated method of checking for these. Such tools can be targeted against Firewalls, servers, networks and operating systems.
- Application Security Analysis Tools: If an organisation is using large integrated business application, key internal controls are highly security dependent. Application level security must be well-designed and built in conjunction with the application's processes and controls.

The CAE should be aware that most of these come with a set of pre-configured rules, or vendor-touted "best practices". Implementation of one will need to be accompanied by a substantive project to create a

rule set that is relevant for that particular organisation. Failure to do so will result in audit reports that contain a number of either false-positives or false negatives.

CAEs should be aware of the following considerations, with respect to IS Audit Accelerators :

- Tools cost money. The CAE should be sure that the benefits outweigh the costs
- That IS Auditors will need to be trained on the new tool. It is not uncommon that a tool sits unused in an Internal Audit Department
- That the tool will need support, patch management and upgrades. Depending on the quality, it may require a standalone server, as well. For this, any tool selection should be managed with the IT department's assistance

Sometimes, IT management or third-party service providers are not allowed tools to access the production environment directly. They are instead asked to do so from a copy of data from an alternative site, or standby server. Any use of tools or scripts should be thoroughly discussed with and approved by IT management and be tested fully before deploying.

(i) **Computer-Assisted Audit Techniques (CAATS)**

IS Auditors can use an appropriate combination of manual techniques and CAATs. IS Audit function needs to enhance the use of CAATs, particularly for critical functions or processes carrying financial or regulatory or legal implications. The extent to which CAATs can be used will depend on factors such as efficiency and effectiveness of CAATs over manual techniques, time constraints, integrity of the Information System and IT environment and level of audit risk.

CAATs may be used in critical areas (like detection of revenue leakage, treasury functions, assessing impact of control weaknesses, monitoring customer transactions under AML requirements and generally in areas where a large volume of transactions are reported).

Process involved in using CAATs involve the following steps :

- Set audit objectives of CAATs
- Determine accessibility and availability of a bank's IS facilities, programs, systems and data
- Define procedures to be undertaken (e.g., statistical sampling, recalculation, or confirmation)
- Define output requirements
- Determine resource requirements: i.e. personnel, CAATs, processing

environment, bank's IS facilities or audit IS facilities

- Obtain access to the bank's IS facilities, programmes, systems and data, including file definitions
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions

CAATs may be used to perform the following audit procedures among others :

- Test of transactions and balances, such as recalculating interest
- Analytical review procedures, such as identifying inconsistencies or significant fluctuations
- Compliance tests of general controls: testing set-up or configuration of the operating system, or access procedures to the programme libraries
- Sampling programmes to extract data for audit testing
- Compliance tests of application controls such as testing functioning of a programmed control
- Re-calculating entries performed by the entity's accounting systems
- Penetration testing

In instances, where CAATs may be used to extract sensitive programmes, system information or production data, IS Auditors should safeguard the programme, system information or production data, with an appropriate level of confidentiality and security. In doing so, IS Auditors should consider the level of confidentiality and security required by the bank, owning the data and any relevant legislation. IS Auditors should be provided with "view access" to systems and data. In case audit procedures cannot be performed in the live environment, appropriate test environment should be made available to IS Auditors. Systems and data under test environment should be synchronised to the live environment.

IS Auditors should use and document results of appropriate procedures to provide for ongoing integrity, reliability, usefulness and security of the CAATs. Example: this should include a review of programme maintenance and change controls over embedded audit software to determine that only authorised changes were made to the CAATs.

In instances where CAATs reside in an environment not under the control of the IS Auditor, an appropriate level of control should, in effect, be placed to identify changes. When the CAATs are changed, IS Auditors should obtain assurance of their integrity, reliability, usefulness and security, through appropriate planning, design,

testing, processing and review of documentation, before placing their reliance.

(j) **Continuous Auditing**

Traditionally, testing of controls performed by an internal audit team was on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach. They included activities such as reviews of policies, procedures, approvals and reconciliations. Today, however, it is recognised that this approach only affords internal auditors a narrow scope, and is often too late to be of "real value" to business performance or regulatory compliance.

Continuous auditing is a method used to perform control and risk assessments automatically on a more frequent basis using technology which is key to enabling such an approach. Continuous auditing changes the audit paradigm from periodic reviews of a sample of transactions to ongoing audit testing of 100 percent of transactions. It becomes an integral part of modern auditing at many levels. It also should be closely tied to management activities such as performance monitoring, scorecard or dashboard and enterprise risk management.

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 analyse key business systems for both anomalies at the transaction level and for data-driven indicators of control deficiencies and emerging risk.

Finally, 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. Depending on the level of implementation and sustenance of risk-based IS Audit approach; banks may explore implementation of continuous auditing in critical areas in a phased manner.

(k) **Application Control Audit**

Detailed pre-implementation application control audits and data migration audits in respect of critical systems needs to be subjected to independent external audit. Banks also need to conduct a post-implementation detailed application control audit. Furthermore, banks should also include application control audits in a risk based manner as part of the regular Internal Audit / IS Audit plans with focus on data integrity (among other factors). General internal auditors with requisite functional knowledge need to be involved along with the IS Auditors in the exercise to provide the requisite domain expertise.

Some of the considerations in application control audit (based on ISACA

guidelines) include :

- i. An IS Auditor should understand the IS environment to determine the size and complexity of the systems, and the extent of dependence on information systems by the bank
- ii. Application-level risks at system and data-level include, system integrity risks relating to the incomplete, inaccurate, untimely or unauthorized processing of data; system security risks relating to unauthorized access to systems or data; data risks relating to its completeness, integrity, confidentiality and accuracy; system-availability risks relating to the lack of system operational capability; and system maintainability risks in terms of adequate change control procedures.
- iii. Application controls to address the application-level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Risks of manual controls in critical areas need to be considered. Where the option to place reliance on programmed controls is taken, relevant general IT controls should be considered, as well as controls specifically relevant to the audit objective. Objectives should be developed to address criteria such as integrity, availability, compliance, reliability and confidentiality. Effectiveness and efficiency can also be additional criteria.
- iv. As part of documenting the flow of transactions, information gathered should include both computerized and manual aspects of the system. Focus should be on data input (electronic or manual), processing, storage and output which are of significance to the audit objective.
- v. Consideration should also be given to documenting application interfaces with other systems. The auditor may confirm the documentation by performing procedures such as a walk-through test.
- vi. Specific controls to mitigate application risks may be identified. Sufficient audit evidence obtained to assure the auditor that controls are operating as intended through procedures such as inquiry and observation, review of documentation and testing of the application system controls, where programmed controls are being tested. Use of computer-assisted audit techniques (CAATs) also needs to be considered.
- vii. Nature, timing and extent of testing should be based on the level of risk to the area under review and audit objectives. In absence of strong general IT controls, an IS auditor may make an assessment of the effect of this weakness on the reliability of the computerized application controls.
- viii. If an IS auditor finds significant weaknesses in the computerized application controls, assurance should be obtained (depending on the audit objective), if possible, from the manually performed processing controls.
- ix. Effectiveness of computerized controls is dependent on general IT controls. Therefore, if general IT controls are not reviewed, ability to place reliance on

controls may be limited. Then the IS Auditor should consider alternative procedures.

- x. Where weaknesses identified during the application systems review are considered to be significant or material, appropriate level of management should be advised to undertake immediate corrective action.

(l) Using the Work of Others

Purpose of an IS Audit standard is to establish and provide a guidance to auditors who can use the work of experts on an audit. The following are standards, to test the reliability of the work of an expert :

- i. IS Auditors should, where appropriate, consider using the work of other experts for audit
- ii. They should assess, and then be satisfied with professional qualifications, competencies, relevant experience, resources, independence and quality control processes, prior to engagement
 - They should assess, review and evaluate work of experts, as a part of an audit, and then conclude the extent of use and reliance of the work
 - They should determine and conclude whether the work of experts is adequate and competent to enable them to conclude on current audit objectives. Such conclusion should be documented
 - They should apply additional test procedures to gain and include scope limitation, where required evidence is not obtained through additional test procedures
 - An expert could be an IS Auditor from external auditing firm, a management consultant, an IT domain expert, or an expert in the area of audit, who has been appointed by management or by the IS Audit Team
 - An expert could be internal or external to the bank. If an expert is engaged by another part of the organisation, reliance may be place on the banks' report. In some cases, this may reduce the need of an IS Audit coverage, though IS Auditors do not have supporting documentation and work papers. IS Auditors should be cautious in providing an opinion on such cases
 - An IS Auditor should have access to all papers, supporting documents and reports of other experts, where such access does not create legal issues. Where access creates legal issues, or such papers are not accessible, auditors should determine and conclude on the extent of use and reliance on expert's work

- The IS Auditor's views, relevance and comments on adopting the expert's report should form a part of the IS Auditor's Report

(m) Third Party Review of Service Providers

A bank may use a third-party service provider (service organisation) to obtain services of packaged software applications and technology environment, which enables customers to process financial and operational transactions (ATM management, networking and infrastructure development and maintenance, document imaging and indexing, software development and maintenance) for which approval may be obtained from NABARD.

Services provided by a third party are relevant to the scope of IS Audit. Especially, when those services and controls within them, are a part of the bank's information systems. Though controls at the service organisation are likely to relate to financial reporting, there may be other controls that may also be relevant to the IS Audit (controls over safeguarding of assets or document images).

A service organisation's services are a part of a bank's information system, including related business processes, relevant to IS Audit if these services affect any of the following :

- * Segments of Information System that are significant to the bank's IS operations
- * Procedures within information system, by which an user entity's transactions are initiated, recorded, processed, corrected (when necessary), transferred to a general ledger and reported, in financial statements
- * The way events and conditions, other than transactions, significant to bank's Information System are captured

IS Auditors will have to obtain an understanding of how a bank uses services of a service organisation in the bank's IS operations, including :

- Nature of services provided by the organisation and significance of those to the bank's information system, including the effect thereof on the bank's internal control
- Nature and materiality of transactions, accounts or financial reporting processes, affected by the service organisation
- Degree of interaction between activities of the organisation and bank
- Nature of relationship between the bank and organisation, including relevant contractual terms for activities undertaken by the organisation

In situations, services provided by the organisation may not appear to be "material" to the bank's IS operations. But, the service nature may be. IS Auditors should determine that an understanding of those controls is

necessary in the circumstances. Information on the nature of services, provided by an organisation, may be available from a variety of sources :

- User manual
- System overview
- Technical manuals
- Contract or service-level agreement between the bank and organisation
- Reports by service organisation, internal auditors, or regulatory authorities, on service organisation controls
- Reports by an auditor of the organisation (service auditor), including management letters

IS Auditors may use a service auditor to perform procedures such as tests of controls at service organisation, or substantive procedures on the bank's IS operations, served by a service organisation.

5 Reporting and Follow-up

This phase involves reporting audit findings to the CAE and Audit Committee. Before reporting the findings, it is imperative that IS Auditors prepare an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses. Additionally, reviewing the actions taken by management to mitigate the risks observed in audit findings and appropriately updating the audit summary memorandum is also important. Reporting entails deciding the nature, timing and extent of follow-up activities and planning future audits.

Professional bodies like ISACA, IIA, ICAI have issued guidance in this regard.

Reporting and follow-up entails following activities or steps :

- Drafting audit summary and memorandum
- Discussing findings with management
- Finalising and submitting reports
- Reviewing the Actions taken report
- Undertaking follow-up procedures
- Archiving documents

These are covered in the following sections :

- (a) **Audit Summary and Memorandum** : An IS Auditor should perform audits or reviews of control procedures and form a conclusion about, and reporting on, the design and operating effectiveness of the control procedures based on the identified criteria. The conclusion for an audit is expressed as a

positive expression of opinion and provides a high level of assurance. The conclusion for a review is expressed as a statement of negative assurance and provides only a moderate level of assurance.

- (b) **Discuss Findings with Management** : Bank's management is responsible for deciding the appropriate action to be taken in response to reported observations and recommendations. IS Auditors are responsible for assessing such management action for appropriateness and the timely resolution of the matters reported as observations and recommendations.

Senior Management may decide to accept the risk of not correcting the reported condition because of cost or other considerations. The Board (or the Audit Committee, if one exists) should be informed of Senior Management's decision on significant observations and recommendations. When Auditors IS believes that an organisation has accepted a level of residual risk that is inappropriate for the organisation, they should discuss the matter with Internal Audit and Senior Management. If the IS Auditors are not in agreement with the decision, regarding residual risk, IS Auditors and Senior Management should report the matter to the Board, or Audit Committee, for resolution.

Events sometimes occur, subsequent to the point in time or period of time of the subject matter being tested, but prior to the date of the IS Auditor's report, that have a material effect on the subject matter and therefore require adjustment or disclosure in the presentation of the subject matter or assertion.

- (c) **Finalise and Submit Reports**

IS Auditors should review and assess the conclusions drawn from the evidence obtained as the basis for forming an opinion on the effectiveness of the control procedures based on the identified criteria.

Major findings identified during an audit should have a definite time line indicated for remedial actions, these should be followed up intensively and compliance should be confirmed.

An IS Auditor's report about the effectiveness of control procedures should cover aspects like :

- Description of the scope of the audit, including :
 - > Identification or description of the area of activity
 - > Criteria used as a basis for the IS Auditor's conclusion
 - > A statement that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management
- A statement that IS Auditors have conducted the engagement to express an opinion on the effectiveness of control

(d) Review Action Taken Report

After reporting of findings and recommendations, IS Auditors should request and evaluate relevant information to conclude whether appropriate action has been taken by management 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. The nature, timing and extent of the follow-up activities should take into account the significance of the reported finding and the impact if corrective action is not taken. The timing of IS Audit follow-up activities in relation to the original reporting should be a matter of professional judgment dependent on a number of considerations, such as the nature or magnitude of associated risks and costs to the entity.

(e) Follow-up Procedures

Procedures for follow-up activities should be established which includes :

- The recording of a time frame within which management should respond to agreed-upon recommendations
- An evaluation of management's response
- A verification of the response, if thought appropriate
- Follow-up work, if thought appropriate
- A communications procedure that escalates outstanding and unsatisfactory responses / actions to the appropriate levels of management
- A process for providing reasonable assurance of management's assumption of associated risks, in the event that remedial action is delayed or not proposed to be implemented
- An automated tracking system or database can assist in the carrying out of follow-up activities.

(f) Update Audit Summary Memorandum

An audit summary memorandum should be prepared and addresses the following :

- Conclusion about specific risk
- Changes in the bank, its environment and banking industry that come to the attention after the completion of the audit planning memorandum and that caused to change audit plan
- Conclusion regarding the appropriateness of the going concern assumption and the effect, if any, on financial statements
- The result of subsequent reviews and conclusion regarding the effect

of subsequent events on financial statements

- Conclusion reached in evaluation of misstatements, including disclosure deficiencies
- If contradiction or inconsistency with final conclusion regarding a significant matter is observed, there should be proper documentation of addressing the inconsistency
- Conclusion of whether the audit procedures performed and the audit evidence obtained were appropriate and consistent to support the audit conclusion

(g) Archival of Documents

Banks are recommended to have an archiving / retention policy to archive the audit results.

Banks to have an archiving policy that :

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

6) Quality Review

This section is aimed at emphasising quality of work of IS Auditors, while performing duties as an auditor. Appropriate levels in IS Audit function are recommended to assess audit quality by reviewing documentation, ensuring appropriate supervision of IS Audit members and assessing whether IS Audit members have taken due care while performing their duties. This will bring efficiency, control and improve quality of the IS Audit.

(a) Evidences and Documentation

IS Auditors may perform the following progressive reviews of the evidences and documentation :

- A detailed review of each working paper prepared by a less-experienced member of the IS Audit team, by a more experienced member, who did not participate in the preparation of such working paper
- A primary review of the evidences and documentation by the Manager or IS Audit Head. Where the manager performs a primary review, this does not require that each working paper be reviewed in detail by the manager, as each working paper has already been reviewed in detail by the person who performed the detailed review.
- An overriding review of the working papers by the CAE, as needed

(b) **Supervision**

IS Audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

(c) **Due Care**

The standard of "due care" is that level of diligence which a prudent and competent person would exercise under a given set of circumstances. "Due professional care" applies to an individual who professes to exercise a special skill such as IS auditing. Due professional care requires the individual to exercise that skill to a level commonly possessed by auditors with the specialty.

Due professional care applies to the exercise of professional judgment in the conduct of work performed. It implies that the professional approaches matters requiring professional judgment with proper diligence. Despite the exercise of due professional care and professional judgment, situations may arise where an incorrect conclusion may be drawn from a diligent review of the available facts and circumstances. Therefore, the subsequent discovery of incorrect conclusions does not, in and of itself, indicate inadequate professional judgment or lack of diligence on the part of the IS Auditor.

Due professional care should extend to every aspect of the audit, including the evaluation of audit risk, the formulation of audit objectives, the establishment of the audit scope, the selection of audit tests, and the evaluation of test results.

In doing this, IS Auditors should determine or evaluate :

- Type and level of audit resources required to meet audit objectives
- Significance of identified risks and the potential effect of such risks on the audit
- Audit evidence gathered
- Competence, integrity and conclusions of others upon whose work IS Auditors places reliance

Intended recipients of audit reports have an appropriate expectation that IS Auditors have exercised due professional care throughout the course of the audit. IS Auditors should not accept an assignment unless adequate skills, knowledge, and other resources are available to complete the work in a manner expected of a professional. IS Auditors should conduct the audit with diligence while adhering to professional standards. IS Auditors should disclose the circumstances of any non-compliance with professional standards in a manner consistent with the communication of the audit results.

(d) **Independent Assurance of the Audit function**

With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, at least once in three years, on the bank's Internal Audit, including IS Audit function, to validate approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Policy.

Objectives of performing a quality assessment are :

- Assess efficiency and effectiveness of an Internal Audit for current and future business goals
- Determine value addition from Internal Audit to the business units Benchmark, identify and recommend, successful practices of Internal Audit
- Assess compliance to standards for professional practice of Internal Audit

Others

As a matter of prudence, banks should rotate IS Auditors in a specific area on periodic basis, say atleast once in two years. The same needs to be incorporated in IS Audit policy / charter. Further, in order to avoid conflict of interest an audit firm / consultant who had provided consulting services on a specific area should not audit the area as part of pre or post implementation audit.
