# CHAPTER 5 : IS AUDIT

**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 judgement in their application, and be prepared to justify any departure therefrom.

*(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 th inherent risks of a business or location and effectiveness of control systems managing inherent risks. In this approach, every bank business or location, including risk management function, undergoes a risk assessment by the internal audit function.

RBI issued the "Guidance Note on Risk-based Internal Audit" in 2002 to all scheduled commercial banks, introducing the system of "risk-based internal audit".

*The guidance note at a broad-level provided the following aspects:*

- Development of a well-defined policy for risk-based internal audit
- Adoption of a risk assessment methodology for formulating risk based audit plan

- Development of risk profile and drawing up of risk matrix taking inherent business risk and effectiveness of the control system for monitoring the risk
- Preparation of annual audit plan, covering risks and prioritisation, 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

Further, while identifying IT risks, an IS Auditor must consider the impact of non-alignment with any information security-related guidelines issued by RBI based on recommendations in Chapter 2 of this report. It should also be ensured that all systems, domains and processes, irrespective of their risk-levels, are covered within a period of **three** years.

### *(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.
*(An illustrative list of areas which can form a part of IS Audit scope are given in Annexure-A.)*

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 for specific areas which also need to be covered in the IS Audit Scope:*

Report of the Committee on Computer Audit (dated: April 2, 2002)
Circular on Information System Audit–A Review of Policies and Practices
(dated: April 30, 2004 (RBI/2004/191 DBS.CO.OSMOS.BC/ 11 /33.01.029/2003-04)

(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 skepticism 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 suditors 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 behavior 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 bank stakeholders:***
1. Frauds involving amounts of Rs 1 crore (and above) should be reported to Special Committee formed to monitor and follow up large fraud cases
2. Other fraud cases should be reported to Fraud Review Councils or independent groups formed to manage frauds
3. The status of fraud cases should be reported to Audit Committee as a part of their review of IS audit
4. IS Auditors should also extend necessary support to Fraud Review Councils or independent groups or Special Committees in their investigations

**(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:*

**1. Enquire and confirm:**

- Search for exceptions and deviations, examine them
- Investigate unusual or non-routine transactions or events
- Check and determine whether something has (not) occurred (sample)
- Corroborate management statements from independent sources
- Interview staff and assess their knowledge and awareness
- Reconcile transactions (e.g., reconciling transactions to bank statements)
- Ask management questions and obtain answers to confirm findings

**2. Inspect:**

- Review plans, policies and procedures
- Search audit trails or problem logs
- Trace transactions through the processes or systems
- Physically inspect presence (documentation or assets)
- Walk-through installations or plans
- Perform a design, or code walk-through

**3. Compare actual with expected findings**

- Observe and describe processes and procedures
- Compare actual with expected behavior

**4. Re-perform or re-calculate:**

- Independently develop and estimate an expected outcome
- Attempt what is prevented
- Re-perform what is detected by detective controls
- Re-perform transactions or control procedures
- Recalculate independently
- Compare expected value with actual value
- Compare actual with expected behavior
- Trace transactions through the processes or systems

**5. Review automated evidenced collection:**

- Collect sample data
- Use embedded audit modules
- Analyse data using computer-assisted audit techniques (CAATs)
- Extract 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 c ontrol 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.

RBI (vide its circular DBS.CO.FrMC.BC.No.7/23.04.001/ 2009-10, dated: September 16, 2009) requires that fraud cases should be reported to law enforcement agencies and to the RBI. Banks should appropriately include requirements for reporting to RBI, of such instances, in engagement letters issued to external IS Auditors.

**(h) Audit Accelerators**

Since IS Audit budgets can be difficult to estimate and manage, CAEs should 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 require an investment, so the CAE should carefully consider the cost or benefits of any solution, prior to investing. 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**

**Electronic Workpapers:** These provide centralised management and retention of workpapers, audit workflow, version tracking, electronic sign-off, etc. It's important to consider the functionality of the tool. For example, can it support multiple simultaneous audits? Prior to implementing any tool, the audit functional requirements should be defined. More important, however, is the content that is provided with the tool. Does it contain suggested audit procedures, or control activities? Internal audit function will need to customise whatever knowledge base is included with the tool, but it can provide a significant headstart.

**Project Management Software:** This schedules workplans, assigns responsibility for tasks, tracks project milestones and deliverables, and can be used by auditors to provide additional consistency and reporting in IS Audits.

**Flowcharting Software:** Can graphically document transaction flows, control points and key process steps. It is useful when documenting process walkthroughs, particularly for detailed application control reviews. Storing graphical process documentation electronically supports the ease of updating flowcharts, as processes change, and provides for easy storage and sharing.

**Open Issue Tracking Software:** This software allows to track outstanding audit issues, or deficiencies, and may also be integrated with document management software. Typically, it includes the ability to assign responsibility for remediation procedures, assign due dates and deliverables, and track and report on progress.

**Audit Department Website:** A number of Internal Audit Departments have established departmental websites that enable central information sharing and communication.

**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, programsmes, 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.

As they implement and sustain the 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). RBI has issued "Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks" (*circular no: DBOD.NO.BP.40/21.04.158/ 2006-07 dated November 3, 2006)*, asking banks to adhere to guidelines before outsourcing activities related to financial services.

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.

Understanding Controls Relating to Services Provided by a Service Organisation

Banks may establish control over the services offered by an organisation, which may be tested by IS Auditors. This may enable IS Auditors to conclude that the bank's controls are operating effectively for some (or all) of the related assertions, regardless of the controls put in place at the organisation. If a bank, for example, uses an organisation to manage payroll transactions, it may establish controls over authentication of submission or receipt of information, which could prevent, or detect, material misstatements.

C*ontrols include:*

- Comparing data submitted to service organisation with reports of information received from it (after the data has been processed)
- Recomputing a sample of payroll amounts for clerical accuracy and reviewing the amount of payroll for reasonableness

Further Procedures When a Sufficient Understanding Cannot Be Obtained from the Bank

An IS Auditor's decision taken on the procedure (individually or in combination) to obtain the necessary information, to provide a basis for identification and assessment of risks of IS operations in relation to a bank's use of a service organisation, may be influenced by several matters.

*They are:*

- Size of both the bank and the service organisation
- Complexity of the transactions (at the bank) and complexity of services provided by the organisation
- Location of the service organisation (e.g., auditors may decide to use another auditor to perform procedures at the organisation on the bank's behalf, if the organisation is in a remote location)
- Whether the procedures are expected to effectively provide auditors with appropriate evidence
- Nature of relationship between the bank and organisation

A service organisation may engage a service auditor to report on the description and design of its controls, and their operating effectiveness, through "Third Party Assurance Reports", such as "Statement of Auditing Standards" (SAS70) based on guidelines provided by the American Institute of Certified Public Accountants (AICPA); or "Standard on Auditing (SA) 402" issued by ICAI. International Auditing and Assurance Standards Board (IAASB) has also issued a new standard "ISAE 3402". AICPA has issued the "Statement on Standards for Attestation Engagements (SSAE) 16", which would replace the current "SAS 70".

These provide a mechanism to the bank's management and statutory auditors to gain assurance on performance of internal control at a service organisation, as they relate to internal control of the user organisation (bank that outsources the work).

**Service organisations:** are entities that provide outsourcing services that impact the control environment of their customers i.e. user organisation. The standards referred above, provide a guidance to service auditors, when assessing the internal control at a service organisation and when issuing a service auditors report: that contain the description, design and operating effectiveness of controls at a service organisation–referred to as a "Type 2 Report".
*It comprises:*
i) A description (prepared by management of the service organisation) of its system; control objectives; related controls; design and implementation at a specified date, or throughout a specified period; and, in some cases, their operating effectiveness throughout a specified period
ii) A report by the service auditor with an objective of conveying reasonable assurance that includes: the service auditor's opinion on the description of the service organisation's system; control objectives and related controls; suitability of control designs to achieve the control objectives; operating effectiveness of controls; and a description of the service auditor's tests of controls and results

In the event of coverage or scope of the service auditor is not per the requirements of the bank, the bank may carry out the audit, or arrange to get the audit done, as per its requirements. A bank may use a service organisation, that in turn, uses a "sub-service organisation" to provide some services that are part of the bank's information system relevant to financial reporting. The "sub-service organisation" may be a separate entity from the "service organisation". Or, it may be related to a service organisation.

IS Auditors may need to consider controls at the sub-service organisation. In situations where one or more sub-service organisations are used, interaction between the activities of a bank and those of the service organisation, is expanded, to include the interaction between the bank, the service organisation and the sub-service organisations. The degree of this interaction, as well as the nature of services provided by the service organisation and the sub-service organisations, are important factors for the user auditor to consider, in determining the significance of the service organisation's and sub-service organisation's controls to the Bank's controls.

**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

**INDUSTRY WIDE RECOMMENDATION**

Accreditation and empanelment of IS audit qualifications or certifications, and IS audit vendors or firms can be considered by Government of India.

**ANNEXURE:**

Annexure A–*Broad scope of IS Audit*

**KEY RECOMMENDATIONS**

1. To meet the responsibility of providing an independent audit function with sufficient resources to ensure adequate IT coverage, the Board or Audit Committee should provide an internal audit function, capable of evaluating IT controls adequately.
2. Banks should enable adequately-skilled Audit Committee composition to manage the complexity of the IS Audit oversight. A designated member of the Audit Committee needs to possess relevant knowledge of Information Systems, IS Controls and audit issues. Designated member should also have competencies to understand the impact of deficiencies, identified in IT Internal Control framework, by IS Audit. The Board or its Audit Committee should seek training to fill any gaps in the knowledge, related to IT risks and controls.
3. Audit Committee should devote appropriate and sufficient time to IS Audit findings identified and members of Audit Committee need to review critical issues highlighted and provide appropriate guidance to the bank's management.
4. Internal Audit is part of the Board's assurance process with regard to the integrity and effectiveness of systems and controls. It is an independent group, with reporting lines directly to the Audit Committee or Board. IS Audit function, being an integral part of Internal Audit function, requires an organisation structure with well-defined roles and responsibilities to function in alignment with the Internal Audit and provide technical audit support.
5. Banks require a separate IS Audit function within the Internal Audit department, led by an IS Audit Head reporting to the Head of Internal Audit or Chief Audit Executive (CAE), assuming overall responsibility and accountability of IS audit function. Where the bank leverages external resources for conducting IS audit on areas, where skills

are lacking within the bank, the responsibility and accountability for such external IS audits still remain with the IS Audit Head and CAE.

6. IS Auditors should act independently of the bank's management. In all matters related to the audit, the IS Audit should be independent of the auditee in both attitude and appearance. IS Auditors should be professionally competent, having skills, knowledge, training and relevant experience to conduct an audit. IS Auditors should exercise due professional care, that includes following professional auditing standards in conducting the audit.
7. 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 IS audits, or insufficient levels of skills/ training of Bank staff. The work outsourced shall be restricted to execution of audits identified in the audit 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.
8. Audit Charter or Policy is a document, which guides and directs activities of an Internal Audit function. IS Audit, being integral part of Internal Audit department, should also be governed by the same Audit Charter or Policy. The mission statement or audit charter should be documented to contain a clear description of mandate, purpose, responsibility, authority and accountability of relevant members or officials in respect of IS Audit, namely the IS Auditors, audit management, and Audit Committee and operating principles. The document should be approved by the board of directors.
9. There should also be annual review of IS Audit Policy or Charter to ensure its continued relevance and effectiveness.
10. The IS Auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys, etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the policy with a view to improving the service or changing service delivery or Audit Charter or Policy, as considered necessary.
11. 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 audit 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.
12. Banks need to carry out IS Audit planning using the Risk Based Audit Approach. It involves an understanding of IT risk assessment concepts and methodology, defining the IS Audit Universe, scoping, and planning the audit, execution and follow up activities. Details in this have been elucidated in the chapter.
13. Executing IS Audit involving 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 workpapers and concluding on tests performed. The detailed requirements have been provided in the chapter.
14. The IS Audit Universe can be built around the four types of IT resources and various IT processes like application systems, information or data, infrastructure(technology and facilities like hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them that enable the processing of the applications) and people (internal or outsourced personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services).

15. The IS Auditor must define, adopt and follow a suitable risk assessment methodology. A successful risk-based IS audit program can be based on an effective scoring system arrived at by considering all relevant risk factors. Banks should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee or the board of directors. Risk assessment related guidelines will vary for individual banks depending on their size, complexity, scope of activities, geographic diversity, and various technologies/systems used.
16. The IS Audit Head is responsible for the annual IS Audit Plan which is prepared based on the scoping document and risk assessment. The Audit plan typically covers the overall audit strategy, scoped audit areas, details of control objectives identified in the scoping stage, sample sizes, frequency/ timing of audit based on risk assessment, nature and extent of audit, IT Resource skills identification and budget allocation. 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.
17. The IS Audit Plan(either separately or as part of overall internal audit plan) should be a formal document, duly approved by the Audit Committee initially and during any subsequent major changes. Audit plan should be prepared so that it is in compliance with any appropriate external requirements in addition to well known IS Auditing Standards.
18. IT governance, information security governance related aspects , critical IT general controls like data centre controls and processes and critical business applications having financial/ compliance/ customer access(like delivery channels) including MIS and regulatory reporting systems need to be audited atleast once a year (or more frequently, if warranted by the risk assessment).
19. IS Auditors should also review critical areas like IT Governance and Information Security Governance structures and practices implemented by the bank, detailed testing of controls on newly development systems before implementing them in live environment (pre-implementation review), performing a post implementation review of application controls (along with underlying IT environment) to confirm that controls as designed are implemented and are operating effectively, reviewing the process followed by implementation team to ensure data integrity upon data migration from older to new system, detailed audit of SDLC process to confirm that security features are incorporated into a new system implemented by the Bank, or while modifying an existing system and validating the IT risks identified by the business teams before launching a new product or service and which may enable the business to incorporate additional controls, if required, in the system before the launch.
20. IS Audits should also cover branches, with focus on large and medium branches, in areas like password controls, control of user ids, operating system security, anti-malware controls, maker-checker controls, segregation of duties, physical security, review of exception reports/audit trails, BCP policy and testing etc
21. Detailed pre-implementation application control audits and data migration audits in respect of critical systems needs to be subjected to independent external audit.
22. 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.
22. IS Auditors should periodically review the results of internal control processes and analyse financial or operational data for any impact on a risk assessment or scoring. Accordingly, various auditee units should be required to keep auditors up to date on all major changes in departments or functions, such as the introduction of a new product, implementation of a new system, application conversions, significant

changes in organisation or staff , new regulatory and legal requirements, security incidents etc.

23. As regards application control audits, application controls to address the application-level risks may be in the form of computerised controls built into the system, manually performed controls, or a combination of both. Risks of manual controls in critical controls 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 various criteria like integrity, availability, compliance, reliability and confidentiality. Effectiveness and efficiency can also be additional criteria.
24. IS Auditors should be reasonably conversant with various fraud risk factors and should assess the risk of occurrence 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 IS Auditors should identify the control objectives and activities that are required to be tested to address fraud risk. The IS Auditor should consider Fraud Vulnerability assessments undertaken by the Fraud Risk Management group, while identifying fraud risk factors in the IT risk assessment process.
25. Banks should consider using testing accelerators — tools and/or techniques that help support the procedures IS Auditors will be performing — to increase the efficiency and effectiveness of the audit. 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 taking into consideration the cost/ benefits of any solution. The audit accelerators can be divided into two general categories – audit facilitators that help support the overall management of the audit (e.g. an electronic workpaper management tool) and testing accelerators that automate the performance of audit tests (e.g. data analysis tools)
26. Auditors need to enhance utilisation of CAATs in various areas such as detection of revenue leakage, assessing impact of control weaknesses, KYC/AML requirements and generally in areas where a large volume and value of transactions are involved. Suitable “read-only” access rights should be provided to auditors for enabling use of CAATs.
27. Banks can consider, wherever possible, for critical systems, continuous auditing approach which 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 can become an integral part of modern auditing.
28. 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.
29. Reporting and follow up aspect of IS Audit involves preparing audit summary and memorandum, requirements for discussing findings with management, finalising and submitting reports, carrying out follow-up procedures, archiving documents and ensuring continuous auditing
30. 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) should be informed of Senior Management’s decision on significant observations and recommendations. When IS Auditors believes that the bank has accepted a level of residual risk that is inappropriate for the organisation, they should discuss the matter with appropriate level of 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.

31. Services provided by a third party are relevant to the IS Audit of a bank when those services, and the controls over them, are part of the bank's information system, including related business processes, relevant to scope of IS Audit. These need to be adequately assessed as part of IS Audit process.
32. With a view to provide assurance to bank's management and regulators, banks are required to conduct a quality assurance, atleast once every three years, on the banks Internal Audit including IS Audit to validate the approach and practices adopted by them in the discharge of its responsibilities as laid out in the Audit Charter / Audit Policy.
33. Accreditation and empanelment of IS audit qualifications/certifications and IS audit vendors/firms can be considered by Government of India.