TG 516 ISA

Committee on Information Technology

The Institute of Chartered Accountants of India

P O Box No. 7100, Indraprastha Marg, New Delhi - 110 002 INDIA

www.icai.org
www.isaicai.org

ISBN 81-88437-60-3

Information Systems Audit Technical Guide

Information Systems Audit

Technical Guide

Committee on Information Technology

The Institute of
Chartered Accountants of India
(Set up under an Act of Parliament)

Information Systems Audit

- Technical Guide

Committee on Information Technology

The Institute of
Chartered Accountants of India

(Set up under an Act of Parliament)

This Technical Guide has been prepared to provide a framework of IS Audit concern areas. The views expressed herein do not necessarily represent the views of the Council of the Institute or any of its Committees.
Also enclosed herewith is a copy of the "RBI Computer Audit Checklist", in the preparation of which the Institute had participated.

First Edition: January 2005

Price: INR120

ISBN No. 81-88437-60-3

E-mail: secyitc@icai.org
www.icai.org
www.isaicai.org

Published by
Dr. Ashok Haldia, Secretary
The Institute of Chartered Accountants of India
PO Box No. 7100
Indraprastha Marg
New Delhi - 110002
INDIA

Design & Realisation
Narendra Bhola

Production
Sterling Preferred Printing
prosterling@gmail.com

Contents

Annexures

Foreword

In the emerging scenario of global village and technological revolution, it is a challenging task for the Institute members to keep abreast with developments and convert threats into challenges and survive/ grow in the globalised world.

The Committee on Information Technology (CIT) has been established to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the threats and challenges ahead. Since its inception, the Committee has proactively considered the modern day requirements and initiated steps to suitably equip the members in terms of knowledge and skills to face the challenges ahead.

There is increasing need for the *Information System Assurance Services* as businesses are increasingly using information technology to service their core business functionality without having sufficient checks and balances leading to increasing business risks. Hence the need for IS Audit by Chartered Accountants with DISA post qualification.

Foreword

There has been an increasing need for a framework for IS Audit. Indeed, it is a pleasure for me to know that the CIT has come out with this informative *Technical Guide on IS Audit*. I am confident that members will be benefited by this timely and sincere effort of the Committee. This publication would contribute to better understanding and dissemination of information in this critical area and members will feel more confident and better equipped to carry out their jobs.

I would like to place on record my deep appreciation for the efforts put in by Shri Harinderjit Singh, Chairman, Committee on Information Technology, members of the committee, for contributing the draft for this publication and Secretary of the Committee for this commendable job.

Sunil Goyal
President

New Delhi
January 24, 2005

Preface

In today's age,there is a seamless integration of business process, internal controls, accounting, systems and IT. In this scenario, our members have to provide assurance and other value add services to clients. With this background, the Committee on Information Technology (CIT) of The Institute of Charetered Accountants of India was established in the year 2000 to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the related challenges ahead. This technical guide is one of the initiatives of the CIT to equip our members to perform the assignments relating to Information Assurance audits and other related value add services The guide contains subjects like an introduction to the IS Audit, IS Audit mandate, defining auditee's requirements, planning for IS Audit, audit risk assessment, documentation, conduct of IS Audit, use and documentation of CAAT. The highlight of the guide is the sample checklists for practical guidance Also included in is a copy of the RBI Checklists for Computer Audit, in the formation of which the ICAI was a member.

Preface

I would like to add a word of caution on use of this technical guide, including checklists.This guide is a generic document that has to be suitably adapted/ tailored to the specific requirements of a particular assignment.

I am grateful to Shri V. Jawahar, Co-opted Member to the Committee on Information Technology, to have contributed the basic draft of this technical guide. In this regard, I also acknowledge the guidance and contribution of our President, Shri Sunil Goyal, FCA, Vice President, Shri Kamlesh S. Vikamsey, FCA, all the members of the Committee on Information Technology and Shri Ravi Arora, Secretary, CIT.

I am sure that this Technical Guide on Information Technology would be of immense help to the members in providing the Information Assurance Services, a value added service, whose demand is on the increase by the day and as usual I look forward to your feedback and suggestions to improve the same.

Harinderjit Singh
Chairman
Committee on Information Technology

New Delhi
January 24, 2005

1 Introduction

Information systems auditing is a function that has been developed to assess whether the computer systems safeguards assets, maintain data integrity and allow the goals of the organization to be achieved effectively and efficiently.

An organisation must control and audit computer based information systems because the costs of errors and irregularities that may arise in these systems can be very high. Sometimes the very existence of the organisation can be severely affected through corruption or destruction of its database, decision making errors caused by poor quality information systems, losses incurred through computer abuse, loss of computer software, hardware and personnel, failure to maintain the privacy of individuals, and failure to control how the computers are used within the organisation.

Computer based systems audit functions do not undermine the importance of traditional internal controls such as separation of duties but are implemented differently. Compared to the manual internal control systems, collecting of evidence on the reliability of internal controls is often more complex in the computer based information systems. Computer controls are often more critical than manual controls.

Evaluation of the reliability of the controls in computer systems is often more complex than in the manual systems. Greater numbers of more complex controls need to be considered. Other sciences such as traditional auditing, computer science, management and behavioural science are the basis of the principles and practice of information systems auditing.

IS Audit Standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively.

The Institute of Chartered Accountants of India has issued AASs covering various aspects. Although these standards are primarily concerned with the audit of financial information, they can be adapted for the purposes of IS Audit depending on its scope and objectives.

The following AASs issued by the Institute of Chartered Accountants of India can be adapted for the IS Audits:

1. Basic Principles Governing an Audit
2. Objective and scope of the Audit of Financial Statements
3. Documentation
4. The Auditor's responsibility to consider fraud and Error in an Audit of financial Statements
5. Audit Evidence

6. Risk Assessment and Internal Controls
7. Relying Upon the Work of an Internal Auditor
8. Audit Planning
9. Using the Work of an Expert
10. Using the Work of Another Auditor
11. Representations by Management
12. Responsibility of Joint Auditors
13. Audit Materiality
14. Analytical Procedures
15. Audit Sampling
16. Going Concern
17. Quality control for Audit Work
18. Audit of Accounting Estimates
19. Subsequent Events
20. Knowledge of Business
21. Consideration of Laws and Regulations in and audit of Financial Statements
22. Initial Engagements Opening Balances
23. Related Parties
24. Audit considerations relating to Using Service Organisations
25. Comparatives
26. Terms of Audit Engagement
27. Communication of Audit Matters With Those Charged with Governance
28. The Auditor's Report on Financial Statements
29. Auditing in a Computer Information Systems Environment
30. External Confirmations
31. Engagements to compile Financial Information
32. Engagements to Perform Agreed upon Procedures regarding Financial Information.

The International Federation of Accountants (IFAC) has issued the following standards relating to auditing in computerized environment:

- 401. Auditing in Computer Information Systems Environment ISA 15.
- Risk Assessment and internal Controls Addendum
- 1008 EDP Characteristics and Considerations to ISA 6.

IFAC has also issued the following IT Guidelines:

1. Managing Security of Information
2. Managing IT Planning for Business Impact
3. Acquisition of IT
4. Implementation of IT Solutions
5. IT Service Delivery and Support

Information System Audit and Control Association (ISACA) (www.isaca.org), an affiliate member of IFAC, has also issued guidelines for IS Auditors. These provide guidelines to IS control professionals for applying standards.

The IS auditors are expected to use their professional judgment when applying the standards, and provide justification (if any) for the departure from the standards.

2 IS Audit Mandate

The IS Auditor must have a clear mandate to perform the IS Audit function. This is usually documented in the audit charter. In case the audit charter exists for the audit function as a whole, the IS mandate should be incorporated.

The Information Systems Audit team usually operates within the overall internal audit function of an organisation. For an internal information systems audit function, an audit charter is prepared for ongoing activities. The audit charter will be subject to an annual review or more often, if the responsibilities are varied or changed. An engagement letter may be used by the internal IS Auditor to further clarify or confirm involvement in specific assignments. For an external IS Audit, an engagement letter is normally prepared for each audit or non-audit assignment. The audit charter or engagement letter should be detailed enough to communicate the purpose, responsibility and limitations of the audit function or audit assignment.

The audit charter or engagement letter should be reviewed periodically to ensure that the purpose, responsibility and scope have not changed. The audit charter should explicitly contain the aspects of authority, responsibility and accountability.
The charter must formally establish the position of the audit function within the organisation and also describe the ways in which it is intended to contribute to the organisation's overall mission and goals.

The charter should state the auditor's right to have access to records, facilities, and personnel in the conduct of their work. The charter must also establish the right of the head of this audit function to have direct access to the Audit Committee and to the Board of Directors.

The charter must also establish the audit functions responsibility in relation to providing advice to the management about how well the organisation is attaining the asset safeguarding, data integrity, effectiveness and efficiency objectives. At the same time it must state that the management has the primary responsibility for controls within an organisation and for taking corrective actions on the basis of the advice of the IS Auditors.

3 Auditee's Requirements

Every time the IS Auditor undertakes the audit function, his mandate must clearly specify the auditee's requirements, based on which he should plan the scope of his work. For example, if the mandate specifies that the audit is required for the network security only. Further the mandate must also specify the objective of the audit e.g. assurance on the controls for physical and logical access, change control process and environmental exposures of the networks.

1. **Scope and limitations**
   The IS Auditor will then plan the scope of his work limiting his audit to all aspects of auditing of network infrastructure security.

2. **Deliverables**
   The mandate must also specify the time frames within which

the various stages of the audit has to be completed and the report expected.

3. **Agreed Fees**

   The audit mandate must also contain the quantum of the fees agreed between the auditor and the organisation.

4. **Intended Recipients**

   The mandate must clearly specify the names and the designations of the persons to whom the audit report must be addressed and sent and also the number of copies that are expected. The audit mandate normally also species the confidentiality to be maintained by the auditor and the audit staff.

5. **Independence**

   IS Auditors should adhere to applicable codes of professional ethics and auditing standards at all times.

   IS Auditors should not participate in an audit if their independence is impaired. For example, independence is impaired if IS Auditors have some expectation of financial gain or other personal advantage due to their influence on the results of the audit.

   However, IS Auditors' independence would not necessarily be impaired as a result of performing an audit of information systems where his/ her personal transactions occur in the normal course of business?

   In order to preserve their independence, IS Auditors should review, among other things:

   - Organisation policies and procedures relating to the independent assurance process.
   - Audit charter, mission statement, policies, procedures and standards, prior reports, and audit plans.
   - The organisational chart.

   The IS Audit plan should define the activities of which the IS Auditor is required to be independent. The IS Auditor's independence of these activities should be regularly monitored by senior management, or by the person who determines and approves the IS Audit plan. This monitoring should include an assessment of the process for assigning individual IS Auditors to specific assignments, to ensure that this process assures independence and sufficient skills.

   Verification of the IS Auditor's adherence to applicable professional codes of conduct should always be carried out. In many circumstances this should be sufficient to provide audit evidence of independence. A revision of the audit plan should be considered if there is an indication that the IS Auditor's independence has been compromised.

   If an IS Auditor continues to be associated with the audit, in circumstances where his independence is impaired, such fact should be disclosed at the appropriate level in his report.

6. **Professional Ethics**

   Every member of the Institute shall adhere to the code conduct and professional ethics of the institute and the guidelines issued by it from time to time.

   Institute members are bound to adhere to such codes and guidelines even in case they hold membership of other professional bodies, international or otherwise.

7. **Due Care**

   IS Auditors must exercise due professional care. Due professional care requires the individual to exercise skill to a level commonly possessed by practitioners of that specialty.

IS Auditors must use common sense and prudent auditing practices with responsible actions. Due diligence means that the IS Auditors must exercise due diligence, which means that they must keep up with these practices in a disciplined way rather than doing them once and letting them fall out of date and becoming useless.

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

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

In doing this, the IS Auditor should determine or evaluate:

a. The type and level of audit resources required to meet the audit objectives.
b. The significance of identified risks and the potential effect of such risks on the audit.
c. The audit evidence gathered.
d. The competence, integrity, and conclusions of others upon whose work the IS Auditor places reliance.

The intended recipients of the audit reports have an appropriate expectation that the IS Auditor has exercised due professional care throughout the course of the audit. The IS Auditor 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.

The IS Auditor should conduct the audit with diligence while adhering to professional standards. The IS Auditor should disclose the circumstances of any non-compliance with professional standards in a manner consistent with the communication of the audit results.

8. Competence

The IS Auditor should be technically competent, having skills and knowledge necessary to perform the audit work.

The IS Auditor should acquire and maintain technical standards and professional competence required to enable him to fulfil his responsibilities effectively.

The IS Auditor is to maintain technical competence through appropriate continuing professional education.

The IS Auditor also should provide reasonable assurance that he/she has access to the relevant technical skill and knowledge to carry out any special assignment that he/she may be asked to attend to.

4 IS Audit Planning

Understanding the Business and IS Requirements
The IS Auditor should develop an audit plan taking into consideration:

- The objectives of the auditee relevant to the audit area, and
- Its technology infrastructure.

Where appropriate, the IS Auditor should also consider the area under review and its relationship to the organisation (strategically, financially and/ or operationally) and obtain information on the strategic plan, including the IS strategic plan.

The IS Auditor should have an understanding of the auditee's information architecture and the auditee's technological direction to be able to design a plan appropriate for the present and, where appropriate, future technology of the auditee.

Terms of reference should be part of the audit plan.

The IS Auditor should carry out a risk assessment and prioritise the identified risks to the extent necessary.

IS Auditors should obtain an understanding of the organisation and its processes, as part of audit planning.

This will assist the IS Auditor in determining the significance of the IS resources being reviewed as they relate to the objectives of the organisation, in addition to giving the IS Auditor an understanding of the organisation's operations and its IS requirements, IS Auditors should also establish the scope of the audit work and perform a preliminary assessment of internal control over the function being reviewed.

The extent of the knowledge of the organisation and its processes required by the IS Auditor will be determined by:

- The nature of the organisation and
- The level of detail at which the audit work has to be performed.

The IS Auditor may require specialized knowledge when dealing with unusual or complex operations. A more extensive knowledge of the organisation and its processes will ordinarily be required when the audit objective involves a wide range of information system functions rather than when the audit objective is for limited functions. For example, a review with the objective of evaluating control over an organisation's payroll system would ordinarily require a more thorough understanding of the organisation than a review with the objective of testing controls over a specific program library system.

The IS Auditor should gain an understanding of the types of events, transactions and practices that can have a significant effect on the specific organisation, function, process or data that is the subject of the auditing project.

Knowledge of the organisation should include the business, financial and inherent risks facing the organisation as well as conditions in the organisation's marketplace. It should also include the extent to which the organisation relies on outsourcing to meet its objectives.

The IS Auditor should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work and considering actions of management, for which the IS Auditor should be alert.

Materiality

In the planning process, the IS Auditor should ordinarily establish levels of materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently. For example, in the review of an existing system the IS Auditor will evaluate materiality of the various components of the system in planning the audit program for the work to be performed.

The IS Auditor should consider both qualitative and quantitative aspects in determining materiality.

Information is material if its misstatement (omission or erroneous statement) could influence the decisions of its users. Materiality depends upon the size and nature of the item, judged in the particular circumstances of its misstatement. The auditor should normally establish levels of materiality such that the audit work will be sufficient to meet the audit objective and will use audit resources efficiently.

Financial auditors generally measure materiality in monetary terms. IS Auditors may audit non-financial items such as physical access controls, logical access controls, program change controls, manufacturing controls, design controls, quality controls, password generation, credit card protection, patient care etc.

IS Auditors should assess the materiality and plan their audit effectively, by focusing their efforts on high risk areas and assess the severity of any errors or weaknesses found.

The assessment of what is material is a matter of professional judgment and includes consideration of the effect on the organization as a whole, of errors, omissions, irregularities and illegal acts which may arise as a result of control weaknesses in the area being audited.

In assessing the materiality, the IS Auditor should consider:

- The aggregate level of error acceptable to the management, IS Auditor, and various regulatory agencies
- Potential for the cumulative effect of minor errors or weaknesses to become material.

Basing on the materiality, the IS Auditor should identify the controls to be examined. With respect to a specific control objective, a material control is a control or group of controls without which control procedures do not provide reasonable assurance that the control objective will be met.

Where the IS Audit objective relates to systems or operations that process financial transactions, the value of the assets controlled by the systems or the value of the transactions processed should be considered in assessing materiality.

In the case of assessing materiality for non-financial transactions ,the following are the examples of measures to assess the materiality:

- Criticality of the business processes supported by the system or operation.
- Cost of the system or operation.
- Potential cost of errors.
- Number of accesses/transactions/inquiries processed per period.
- Nature, timing and extent of reports prepared and files maintained.

- Nature and quantities of materials handled.
- Service level agreements requirements and cost of potential penalties.
- Penalties for failure to comply with legal and contractual ,public health and safety requirements.

5 Risk Assessment

The level of audit work required to meet a specific audit objective is a subjective decision made by the IS Auditor. There are two types of risks that an IS Auditor faces, the risk of reaching an incorrect conclusion based on the audit findings (audit risk) and the risk of errors occurring in the area being audited (error risk).

Selection of a Risk Assessment Methodology

An IS Auditor may chose from the many computerized and non-computerized risk assessment methodologies that are available. These methodologies range from those that classify risks as high, medium and low to those that involve complex and apparently scientific calculations to provide a numeric risk rating.

While selecting the methodology to be used, the IS Auditor considers the level of complexity and detail appropriate to the organisation being audited.

The IS Auditors have to use subjective judgments in all risk assessment methodologies. Hence the auditor should identify the subjective decisions required for a particular methodology and also consider whether these judgments can be made and validated to an appropriate level of accuracy.

While deciding the most appropriate risk assessment methodology to use, an IS Auditor considers the following:

- The type of information required to be collected (some systems use financial effect as the only measure which may not always appropriate for IS Audits)
- The cost of software or other licenses required to use the methodology.
- The extent to which the information required is already available.
- The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise).
- The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and/or effectiveness of their audits.
- The willingness of management to accept the methodology as the means of determining the type and level of audit work carried out.

Since the conditions affecting the audits may change over time, no risk assessment methodology can be expected to be appropriate in all situations and times. The IS Auditor should therefore re-evaluate the chosen risk assessment methodology.

Use of Risk Assessment

An Is auditor should use the selected risk assessment methodology in combination with other audit techniques in developing the

overall audit plan and making planning decisions such as:

- The nature, extent, and timing of audit procedures.
- The areas or business functions to be audited.
- The amount of time and resources to be allocated to an audit.

The IS Auditor should consider each of the following types of risk to determine their overall level:

- Inherent risk.
- Control risk.
- Detection risk.

Documentation

The IS Auditor should document the risk assessment methodology used for an audit. This should ordinarily include:

- A description of the risk assessment methodology used.
- The identification of significant exposures and the corresponding risks.
- The risks and exposures the audit is intended to address.
- The audit evidence used to support the IS Auditor's assessment of risk.

Assessment of Internal Controls

Any IS Audit should include assessment of the internal controls either as a part of the audit subject or as a basis for reliance being gathered as a part of the audit.

Where the objective is evaluation of internal controls the IS Auditor should consider the extent to which it will be necessary to review such controls.

When the objective is to assess the effectiveness of controls over a period of time, the audit plan should include procedures appropriate for meeting the audit objectives, and these procedures should include compliance testing of controls.

When the objective is not to assess the effectiveness of controls over a period of time, but rather to identify control procedures at a point in time, compliance testing of controls may be excluded.

When the IS Auditor evaluates internal controls for the purpose of placing reliance on control procedures in support of information being gathered as part of the audit, the IS Auditor should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation.

During a review, the IS Auditor will consider the appropriateness of this evaluation in determining the extent to which controls can be relied upon during testing. For example, in using computer programs to test data files, the IS Auditor should evaluate controls over program libraries containing programs being used for audit purposes to determine the extent to which the programs are protected from unauthorised modification.

Determination on the Extent of Audit

Before an IS Auditor commences the work, a preliminary review program should be completed. Such program should be documented in a manner that will permit the auditor to record completion of the audit work and identify the work that remains to be done.

During the course of an audit, the auditor should evaluate the adequacy of the program based on the information gathered. In circumstances when the auditor determines that the planned procedures are inadequate, the IS Auditor should modify the program accordingly.

The IS Auditor should include management of the personnel resources required in the audit plan, based on the audit resources requirement.

The IS Auditors should ensure that the audit plan is in compliance with any external requirements in addition to the auditing standards and guidelines.

Apart from listing the work to be done, the IS Auditor should, to the extent practicable, prepare a list of personnel and other resources required to complete the work, a work schedule, and a budget.

IS Auditors must always consider changes in the audit program based on the evaluation of the adequacy of the program and the preliminary findings.

6 Plan Documentation

Planning is the first step in an IS Audit. IS Auditors must ensure that they exercise "due care" right from the point of planning an audit. The IS Audit is normally planned preferably by means of a flow chart. IS Auditors normally follow the following steps for conducting an IS Audit:

1. Preliminary audit work.
2. Obtain an understanding of the control structure.
3. Assess control Risk.
4. Decide whether to rely on the controls or to undertake extended substantive testing.
5. Testing of controls.
6. Reassess control risk or decide to undertake extended substantive testing.
7. Undertake limited substantive testing.
8. Forming an audit opinion.
9. Reporting.

Plan Endorsement by Auditor and Auditee

Once the audits plan has been made, both the auditor and the auditee must endorse it. The endorsement of the plan by the auditee is important because it then ensures the availability of resources from the organisation for the smooth and speedy completion of the audit. Endorsement also gives the IS Auditor authority to conduct the audit within the scope as required by the auditee, at the same time allowing the IS Auditor the freedom to undertake important tests such as management controls not specifically within the scope of the audit.

Preliminary Audit Program

Before starting the audit, the IS Auditor undertakes a preliminary audit program. The preliminary audit program should consist of the following:

1. Identify the technical skills and resources needed for the audit.
2. Identify the sources of information for test or review such as functional flowcharts, policies, standards, procedures, and prior audit papers.
3. Identify locations and facilities to be audited.
4. Identify and select the audit approach to verify and test the controls.
5. Identify a list of individuals to interview.
6. Identify and obtain departmental policies, standards, and guidelines for review.
7. Develop audit tools and methodology to test and verify control.

Planning of Audit Resources and Allocation of Work

1. The IS Auditor must plan their resources to effectively achieve the objectives of the audit in an efficient manner
2. The IS Auditors must therefore decide on various issues like:
   a) The number of personnel to be deployed for the audit.
   b) The personnel who shall interview the management.
   c) The personnel who shall review the standards, procedures and the guidelines.

d) The personnel who shall conduct various tests e.g. penetration testing.

In case the IS Auditor does not have in the team, personnel having skills to conduct highly technical tests, he may have to use the services of experts. Here the decision has to be taken on who/ when/ where etc. At the same time the budget has to be kept in mind.

The IS Auditors also must clearly decide on the use of various audit tools, if there is a need for the use of such tools.

The IS Auditor should at all times document the circumstances and the reasons for all the decisions taken.

All the audit personnel must be given clear instructions along with the purpose of the audit, so that the final objective of the audit is always in sight.

Evaluation and Modification of the Audit Program Based on Initial Findings

After developing the audit program and gathering audit evidence, the information gathered should be evaluated in order to develop an audit opinion.

The IS Auditor must consider all the strengths and weaknesses, and develop audit opinions and recommendations. The IS Auditor makes judgments that are often based on experience rather than from reference materials. Professional care is particularly essential in evaluating audit strengths and weaknesses.

The IS Auditor should asses the results of the evidence gathered for compliance with the control objectives established during the planning stages.

A control matrix is often utilized in assessing the proper level of controls. The matrix works by placing known types of errors that can occur in the area under review on the top axis and the known controls to detect or correct the errors on the side axis. Then using the ranking method, the matrix is filled using the appropriate measurement. When completed the matrix illustrates areas where controls are weak or lacking.

The IS Auditor may find a variety of strong and weak controls. The IS Auditors must implement compensating controls where controls have been identifies as weak.

A control objective will not normally be achieved by considering on control adequate. Rather, the IS Auditor should perform a variety of testing procedures and evaluate how these relate to one another. An IS Auditor should always review compensating controls prior to reporting a control weakness.

The IS Auditor may not find each control procedure to be in place but should evaluate the totality of control by considering the strengths and weaknesses of control procedures.

Determination of the Tools to be Used

The IS Auditor should have a thorough understanding of computer assisted audit techniques (CAATs) and know where and when to apply them. CAATs are significant tools for the auditor to gather information independently. They provide a means to gain access and to analyse data for a pre-determined objective and to report the audit findings with emphasis on the reliability of the records produced and maintained in the system.

The following are some examples of CAATs which can be used by IS Auditors, to collect evidence:

- Generalised audit software - ACL/ IDEA.
- Utility software.
- SQL commands.

- Third party access control software.
- Application systems.
- Options, reports built into the system.

Evidence

Evidence is any information used by the IS Auditor to determine whether the entity or data being audited follows the established audit criteria or objectives. Audit evidence may include the IS Auditors observations, notes taken from interviews, material extracted from correspondence and internal documentation or the results of audit test procedures. While all evidence will assist the IS Auditor in developing audit conclusions, some evidence is more reliable than others. While evaluating the evidence, IS Auditors should keep the following points in mind:

- Independence of the provider of the evidence.
- Qualifications of the individual providing the evidence.
- Objectivity of the evidence.

The IS Auditor should apply good judgment to determine which material is directly appropriate to the objectives of the audit and which is not relevant. Both quality and quantity of evidence must be assessed by the IS Auditor. These two qualities are referred to as competent (quality) and sufficient (quantity). Evidential matter is competent when it is valid and relevant. Audit judgment is used to determine when sufficiency is achieved in the same manner that is used to determine the competency of evidential matter.

Gathering of evidential matter is the key step in the audit process. The IS Auditor should be aware of the various forms of evidence and how evidence is gathered and reviewed.

The IS Auditors normally use the following techniques for gathering evidence:

- Reviewing information systems organisation structures.
- Reviewing information systems documentation standards.

- Interviewing appropriate personnel.
- Observing processes and employee performance.

Sampling

IS Auditors use sampling when time and cost considerations preclude a total verification of all transactions or events in a predefined population. The population consists of the entire group of items that need to be examined. The subset of the population members is called a sample. Sampling is used to infer characteristics about a population, based on the results of examining the characteristics of a sample of the population.

There are two general approaches to audit sampling statistical and non statistical. Within these two general approaches they are two primary methods that are used by the auditors, attribute sampling and variable sampling.

Attribute sampling, generally applied in compliance testing situations, deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable samples, generally applied in substantive testing situation, deals with population characteristic that vary, such as rupees and weights, and provides conclusion related to deviation from the norms.

Attribute sampling refers three different, but related types of proportional sampling.

1. Attribute sampling is sampling model that tires to estimate the rates (percent) of occurrence of specific quality (attribute) in a population.
2. Stop and go sampling is a model that helps prevent excessive sampling of an attribute by allowing an audit test to be stopped at the earliest possible moment. It is used when the IS Auditors believes that relatively few errors will be found in a population.
3. Discovery sampling is the model that can be used when the expected occurrence rate is extremely low. This model is used

when the objective of the audit is to seek out fraud, circumvention of regulation are other irregularities.

Variable sampling refers to a number of different types of quantitative sampling models:

1. Stratified mean per unit model is one in which the population is divided into groups and samples are drawn from various groups.
2. Un-stratified mean per unit model is one where by a sample mean is calculated and projected as an estimated total.
3. Difference estimation model is used to estimate the total difference between the audited values and the unaudited values based on differences obtained from sample observations.

The main steps used by an IS Auditor in the construction and selection of a sample for an audit test include:

1. Determining the objectives of the test.
2. Defining the population to be sampled.
3. Determining the sampled method i.e. attribute versus variable.
4. Calculating the sample site.
5. Selecting the sample.
6. Evaluating the sample from audit perspective.

7 Documentation

Contents

IS Auditors must maintain proper documentation of their work as these are the record of the work performed by them and the evidence supporting their findings and conclusions. Documentation is meant to:

- Prove the extent to which an IS Auditor has complied with guidelines and standards.
- Assist in the planning, performance and review of audits.
- Facilitate third party reviews.
- Evaluate the quality assurance program of the IS Audit function.
- Extend support in circumstances such as insurance claims, fraud cases and lawsuits.
- Assist in the professional development of the staff.
- IS Auditors must ensure that at least the minimum level of documentation is maintained as a record of the planning and preparation of the audit scope and objectives.

- Audit program.
- Audit steps performed and the evidence gathered.
- Audit conclusions, findings and recommendations.
- Report issued.
- Supervisory review.

The extent of the documentation maintained by an IS Auditor depends on the needs of the audit and would normally include:

- The IS Auditors understanding of the area to be audited and its environment.
- The understanding of the information processing systems and the internal control environment.
- The author and source of the audit documentation and the date of completion.
- Audit evidence, its source and the date of completion.
- The auditees response to recommendations.

IS Auditors must ensure that the documentation they maintain includes information required by standards and guidelines issued by the professional bodies like ICAI, ISACA, ISC2 etc., law, government guidelines, and that such documentation is clear, complete and understandable by the reviewer.

Custody, Retention and Retrieval

IS Auditors must ensure that the legal, professional and organizational requirements as to the period of custody and retention of the documentation that support audit findings are properly adhered to, and that there are proper policies and procedures in place for such custody and retention.

IS Auditors must also ensure that the documents are organized, stored and secured in a manner appropriate for the media on which it is retained and should be retrievable for a time sufficient to satisfy the policies and procedures as mentioned above.

8 Use of Computer Assisted Auditing Techniques

There is an increasing need to use Computer Assisted Audit Techniques(CAAT)/ Generalised Audit Software in normal audits, more so for IS Audits considering the need to audit mammoth number of transactions. CAATs include generalized audit software, such as:

- ACL/ IDEA.
- Utility software.
- Test data.
- Application software for continuous online auditing and expert system.

The IS Auditor must have an understanding of the capabilities and limitations of the CAATs so that the same may be used effectively and efficiently. Before utilising CAATS, an IS Auditor must document the need and also how the use of CAATs would serve the objective of the audit.

Utility software provides evidence to the auditors about system control effectiveness. It is generally a subset of software, for example database management system's generated report. IS Auditors use test data to assess whether logic error exists in a program and whether the program meets it objectives? A review of an application system will provide information about internal controls built in the system to an IS Auditor. IS Auditors use expert systems because the query base system is built on the knowledge base of the senior auditors or managers and gives direction and valuable information while carrying out the audit.

Generalised audit software refers to standard software that has the capability to directly read and access various database platforms, flat file systems and ASCII formats.

IS Auditors normally use generalized audit software for the following functions:

- File access Enables the reading of different record format and file structures.
- File reorganization- enables an indexing, sorting, merging and linking with another file to get meaningful inferences
- Data selection - Enables global filtration condition and selection criteria.
- Statistical functions Enable sampling, stratification and frequency analysis.
- Arithmetical functions Enable arithmetic operators and functioning.

While using CAATs, the IS Auditor must consider the following concerns.

- The integrity reliability and security of the CAATs.
- The integrity of the information systems and security environment.
- The confidentiality and security of the data as required by the client.

Continuous Online Audit Approach

CAATs have the ability to improve audit efficiency, particularly in paperless environment through continuous online auditing techniques. The IS Auditor must develop audit techniques that are appropriate for use with advanced computerized systems. IS Auditors may use one or more of the following five types of automated evaluation techniques:

1. **Systems Control Audit Review File (SCARF) and Embedded Audit Modules (EAM)**: The use of this technique involves embedding specially written audit software in the organization's host application system so that the application systems are monitored on a selective basis.

2. **Snapshots:** This technique involves taking what might be termed pictures of the processing path that a transaction follows from the input to the output stage. With the use of this technique, transactions are tagged by applying identifiers to input data and recording selected information about what occurs for the auditor's subsequent review.

3. **Audit hooks:** This technique involves embedding hooks in application systems to function as red flags and induce IS Auditors to act before an error or irregularity gets out of hand.

4. **Integrated Test Facilities (ITF)**: In this technique facilities are set up and included in an auditee's production files. The IS Auditor can make the system process either live transactions or test transactions during regular processing runs and have these transactions update the records of the dummy entity. The operator enters the test transactions simultaneously with live transactions that are entered for processing. The auditor then compares the output with the data that have been independently calculated to verify the correctness of the computer processed data

5. **Continuous and Intermittent Simulation (CIS):** The computer system, during a process run of a transaction, simulates the instruction execution of the application. As each transaction is entered, the simulator decides whether the transaction meets certain predetermined criteria and if so, audits the transaction. If not, the simulator waits until it encounters the next transaction that meets the criteria.

While deciding the use of CAATs, the IS Auditors must consider which of the following advantages would help in achieving the objectives of the audit:

- Reduced level of audit risk.
- Greater independence from the auditee.
- Broader and more consistent audit coverage.
- Faster availability of information.
- Improved exception identification.
- Greater flexibility of run times.
- Greater opportunity to quantify internal control weaknesses.
- Enhanced sampling.
- Cost savings over time.

Like any other process, an IS Auditor should weigh the costs/benefits of CAATs before going through the effort, time and expense of purchasing or developing them.

The IS Auditor must also consider the following issues when taking a decision of the use of CAAT's.

- Ease of use, both for existing audit staff and future staff.
- Training requirements.
- Complexity of coding and maintenance.
- Flexibility of uses.
- Installation requirements.
- Processing efficiencies (especially with a PC CAAT).
- Effort required in bringing the data files and their co-relation into the CAATs for analysis.

- Level of audit risk.
- CAATs may produce a large proportion of the audit evidence developed on IS Audits and, as a result, the IS Auditor should carefully plan for and exhibit due professional care in the use of CAATs.

Planning Steps

The major steps to be undertaken by the IS Auditor in preparing for the application of the selected CAATs are:

- Set the audit objectives of the CAATs.
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data.
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.).
- Define output requirements.
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities).
- Obtain access to the organisation's IS facilities, programs/system, and data, including file definitions.
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions.

Arrangements with the Auditee

Data files, such as detailed transaction files, are often only retained for a short period of time; therefore, the IS Auditor should make arrangements for the retention of the data covering the appropriate audit time frame.

Access to the organisation's IS facilities, programs/system, and data, should be arranged for well in advance of the needed time period in order to minimise the effect on the organisation's production environment.

The IS Auditor should assess the effect that changes to the production programs/system may have on the use of the CAATs. In doing so, the IS Auditor should consider the effect of these changes on the integrity and usefulness of the CAATs, as well as the integrity of the programs/system and data used by the IS Auditor.

Testing the CAATs

The IS Auditor should obtain reasonable assurance of the integrity, reliability, usefulness, and security of the CAATs through appropriate planning, design, testing, processing and review of documentation before placing reliance upon the CAATs. The nature, timing and extent of testing is dependent on the commercial availability and stability of the CAATs.

Security of Data and CAATs

Where CAATs are used to extract information for data analysis the IS Auditor should verify the integrity of the information system and IT environment from which the data are extracted.

CAATs can be used to extract sensitive program/system information and production data that should be kept confidential.

The IS Auditor should safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the IS Auditor should consider the level of confidentiality and security required by the organisation owning the data and any relevant legislation.

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

When the CAATs reside in an environment not under the control of the IS Auditor, an appropriate level of control should be in effect to identify changes to the CAATs. When the CAATs are changed, the IS Auditor should obtain assurance of their integrity, reliability, usefulness, and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs.

Mandate to Use CAATs

IS Auditors should take care to mention the use of CAATs in their Audit Mandate, if required, to avoid issues/ problems later and ensure availability of data for analysis.

9 Performance of Audit Work

Gathering Audit Evidence

The use of CAATs should be controlled by the IS Auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. The IS Auditor should:

- Perform a reconciliation of control totals if appropriate.
- Review output for reasonableness.
- Perform a review of the logic, parameters or other characteristics of the CAATs.
- Review the organisation's general IS controls which may contribute to the integrity of the CAATs (e.g., program change controls and access to system, program, and/or data files)

Generalised Audit Software

When using generalised audit software to access the production data, the IS Auditor should take appropriate steps to protect the integrity of the organisation's data. With embedded audit software, the IS Auditor should be involved in system design and the techniques will have to be developed and maintained within the organisation's application programs/systems.

Utility Software

When using utility software, the IS Auditor should confirm that no unplanned interventions have taken place during processing and that the utility software has been obtained from the appropriate system library. The IS Auditor should also take appropriate steps to protect the integrity of the organisation's system and files since these utilities can easily damage the system and its files.

Test Data

When using test data, the IS Auditor should be aware that test data only point out the potential for erroneous processing; this technique does not evaluate actual production data. The IS Auditor also should be aware that test data analysis can be extremely complex and time consuming, depending on the number of transactions processed, the number of programs tested, and the complexity of the programs/system. Before using test data the IS Auditor should verify that the test data will not permanently affect the live system.

Application Software Tracing and Mapping

When using application software tracing and mapping, the IS Auditor should confirm that the source code being evaluated tallies with the generated the object program currently being used in production. The IS Auditor should be aware that application software tracing and mapping only points out the potential for erroneous processing; it does not evaluate actual production data.

Audit Expert Systems

When using audit expert systems, the IS Auditor should be thoroughly knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment/situation.

10 CAATs Documentation & Relying on Experts

Work Papers

The step-by-step CAATs process should be sufficiently documented to provide adequate audit evidence. Specifically, the audit work papers should contain sufficient documentation to describe the CAATs application, including the details set out in the following sections.

Planning

Documentation should include:

- CAATs objectives.
- CAATs to be used.
- Controls to be exercised.
- Staffing and timing.

Execution

Documentation should include:

- CAATs preparation and testing procedures and controls.
- Details of the tests performed by the CAATs.
- Details of inputs (e.g., data used, file layouts), processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports).
- Listing of relevant parameters or source code.

Audit Evidence

Documentation should include:

- Output produced.
- Description of the audit analysis work performed on the output.
- Audit findings.
- Audit conclusions.
- Audit recommendations.

Reporting

Reporting must describe the CAATs used and objectives served. The objectives, scope and methodology section of the report should contain a clear description of the CAATs used. This description should not be overly detailed, but it should provide a good overview for the reader.

The description of the CAATs used should also be included in the body of the report, where the specific finding relating to the use of the CAATs is discussed.

If the description of the CAATs used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report and the reader referred to an appendix with a more detailed description.

Use of Work of Another Auditor/ Expert

Rights of Access: The IS Auditor should ensure that, where the work of other auditors or experts is relevant to the IS Audit objectives, the audit charter or engagement letter specifies the IS

Auditor's right of access to this work.

Planning - Planning Considerations: When an IS Audit involves using the work of other auditors or experts, the IS Auditor should consider their activities and their effect on the IS Audit objectives while planning the IS Audit work. The planning process should include

- Assessing the independence and objectivity of the other auditors or experts.
- Assessing their professional competence.
- Obtaining an understanding of their scope of work and approach.
- Determining the level of review required.

Independence and Objectivity

The processes for selection and appointment, the organisational status, the reporting line and the effect of their recommendations on management practices are indicators of the independence and objectivity of other auditors and experts.

Professional Competence

The qualifications, experience and resources of other auditors and experts should all be taken into account in assessing professional competence.

Scope of Work and Approach

Scope of work and approach ordinarily will be evidenced by the other auditor's or expert's written audit charter, terms of reference or letter of engagement.

Level of Review Required

The nature, timing and extent of audit evidence required will depend upon the significance of the other IS Auditor's or expert's work. The IS Auditor's planning process should identify the level of review which is required to provide sufficient reliable, relevant and useful audit evidence to achieve the overall IS Audit objectives effectively. The IS Auditor should consider reviewing the other auditor's or expert's final report, audit programme(s) and audit work papers. The IS Auditor should also consider whether supplemental testing of the other auditor's or expert's work is required.

Review of Other Auditor's or Expert's Work papers

Where a review of the other auditor's or expert's work papers is necessary, the IS Auditor should perform sufficient audit work to confirm that the other auditor's or expert's work was appropriately planned, supervised, documented and reviewed and to consider the appropriateness and sufficiency of the audit evidence provided by them. Compliance with relevant professional standards should also be assessed.

Review of Other Auditor's or Expert's Report(s)

The IS Auditor should perform sufficient reviews of the other auditor's or expert's final report(s) to confirm that the scope specified in the audit charter, terms of reference or letter of engagement has been met, that any significant assumptions used by the other auditors or experts have been identified and that the findings and conclusions reported have been agreed by management.

It may be appropriate for management to provide their own report on the audited entities, in recognition of their primary responsibility for systems of internal control. In this case the IS Auditor should consider the management's and auditor's report together.

The IS Auditor should assess the usefulness and appropriateness of reports issued by the other auditors and experts, and should consider any significant findings reported by the other auditors or experts. It is the IS Auditor's responsibility to assess the effect of the other auditor's or expert's findings and conclusions on the overall audit objective, and to verify that any additional work required to meet the overall audit objective is completed.

11 Reporting on Audit Work

FOLLOW-UP ACTIVITIES

Implementation of Recommendations

Where appropriate, the IS Auditor should consider the extent to which management has implemented any recommendations of the other auditor or expert.

REPORTING

Intended Recipients

The IS Auditor must consider the needs of the intended recipients of the report. These may include the auditee, the executive management, the board of directors or its audit committee, and the government.

Style and Content

The style and content of the report must be appropriate to the intended recipients and may be written, oral or in any other form.

Every report should identify the organisation and include a title, the date and should be appropriately authenticated.

Reports should be objective, concise, constructive and timely.

Statement of Objectives

Every report should clearly state the objective of the audit to identify what the audit was intended to accomplish. In case the audit objective has not been accomplished, then the IS Auditor must state the fact in his report.

Scope, Nature Timing and Extent of Audit

IS Auditors must include in their reports the scope of the audit that describes the nature, timing, and extent of the audit work performed. The scope should identify the functional area of audit, the audit period covered and the information systems, applications or processing environments audited.

The report must also state the circumstances of scope limitation when in the auditors' opinion, appropriate tests and procedures could not be completed or when the auditee has imposed restrictions on the audit work.

Restriction on Distribution

The report should identify the auditee and indicate the issue date. If necessary, the report should specify that it is solely for the information of the intended recipient such as the auditee, management, government etc. The report must also state any restrictions on its distribution.

Significant Findings to be Reported

The report must include all significant findings, and when any finding requires explanation, the IS Auditor should describe its cause and its risk. In appropriate circumstances the IS Auditor should provide his explanation in a separate document and make reference to it in the report. The IS Auditor should also identify the organizational, professional and governmental criteria applied (such as the guidelines issued by the ICAI, the standards and guidelines issued by ISACA or the COBIT issued by ISACF).

Conclusion

The IS Auditors evaluation of the area being audited should be expressed as a conclusion. The conclusion may be an overall evaluation or multiple evaluations related to a specific audit objective.

Recommendations

The audit report must express recommendations for corrective action and these should be linked with specific findings.

Qualifications

The report should clearly state any significant qualifications or reservations.

Presentation

The report should be presented in a logical and organized manner and should contain sufficient information to be understood by the intended recipients.

Timeliness

The report should be issued in a timely manner so as to enable prompt corrective action. The IS Auditor may communicate significant findings prior to the issuance of his report, but such communications should not alter the intent and content of the report.

Subsequent Events

The IS Auditor must consider all material changes in the organisation or environment between the time of completion of the audit and the issuance of the final version of the report, which would affect the reported findings, conclusions and recommendations. In case of any such changes, the IS Auditor must alert the recipients of the report to the potential effect of these changes on the reported findings, conclusions and recommendations.

Annexures

Annexures

Annexure 1

Sample Checklist for Risk Assessment

A. BACKGROUND

Control Objective

To determine general factors related to the site location and its history, which might have an impact on the exposures and risks to that site.

1. History of the Location

- What is the 'history' of this location? Previous exposures, threats from historical records.
- Review available reports, local emergency data.

2. Critical Dependencies

- Why is this site considered to be a critical one (to the organization)?
- Is it owned or leased? If leased, who is the landlord?
- What are the critical dependencies (for the company) on this

particular location?

- If this site is (or contains) a data centre or network operations centre, what critical business functions/ applications are processed? What is the 'window' (time frame) for recovery purposes (should a disaster strike)?

3. Key Vendors/ Suppliers (Capabilities/ Impact)

- List the names of key vendors as well as the services and/ or products they provide to this site (utilities, hardware/ software suppliers, etc.).
- What is the dependency level? How critical is each one?
- What is the experience level, how reliable, are there any problems? (Strengths/ weaknesses of each Vendor).

4. Insurance Coverage

- Who is the insurance provider? Self-insured?
- What coverage? Property, liability, etc.
- Business interruption coverage?
- What are the deductibles?

B. WRITTEN PROCEDURES

Control Objective

To ensure that documentation covering physical security procedures clearly and adequately reflects the commitment made by management to this requirement, and that these procedures are properly communicated to, and followed by, the appropriate personnel at this facility.

- Review written procedures covering physical security
- In what format are they documented?
- Who has copies of the procedures?
- Who has overall responsibility for physical security at this facility?
- Who is responsible for documentation? Dissemination?
- Are other areas of responsibility documented?
- Are all departments/ locations involved?

- Are individual/ group responsibilities/ accountabilities documented?
- How is compliance (with written procedures) measured?
- What is the method for updating procedures/ maintaining documentation currency?
- Are there procedures for periodic physical security reviews, tests?
- Are checklists, inventory lists, control lists used? Are they maintained and communicated?
- Is there a physical security awareness program? How are physical security procedures communicated?
- Is there an Employee Handbook? Are physical security procedures referenced?
- Are there written procedures covering the return of co-owned items upon employee termination?

C. PROTECTION OF PERSONNEL

Control Objective

To ensure that employees and other on site personnel are protected from potential hazards at the facility.

- Are employees trained in using on-site fire-fighting equipment, shutting down equipment, reporting emergencies and evacuation procedures?
- Are employee protection/EPR (Emergency Preparedness and Response) procedures documented and communicated to all employees on a regular basis?
- Are there formal employee notification procedures in place (in the event of disaster)? Are telephone trees used to communicate during off duty hours?
- Are employees aware of individuals on site who have First Aid/ CPR Training? Are there adequate emergency exits/ routes/ lighting/ alarms? Are there "crash bars" on the emergency exit doors? Are these doors accessible from the outside? Do access doors "fail open" in emergency?
- Are emergency exits/ routes/ lighting/ alarms checked/ tested on a periodic basis?

D. FIRE PROTECTION

Control Objective

- To ensure that the building, offices, and processing environment are adequately protected from major fire.

1. Building Construction

- Is the building suitably constructed to reduce the potential for fire?
- Exterior/interior walls? Rooms? Closets?
- What is the potential for hazards in the vicinity of the building (exterior) i.e., power lines, barriers, which could restrict access of fire department and/or emergency services personnel?
- Are there any housekeeping related hazards?
- What is the status of smoke/fire detectors, alarms? How often are they tested?

2. Computer Room Construction

- Is the computer room constructed to IAW industry standards? (e.g., NFPA)
- Are adjacent areas free from highly flammable materials?
- Are external building air/heat ducts which enter the computer room lined with non-combustible materials and equipped with power dampers to prevent/minimize smoke migration?
- Is the computer room equipped to minimize the extent of fire damage?

3. Magnetic Media Library

- Is the on-site magnetic media library constructed to IAW industry standards? (E.g., NFPA)
- Are adjacent areas free of highly flammable materials?
- Are external building air/heat ducts (which enter the tape library) lined with non-combustible materials and equipped with power dampers to prevent smoke migration?
- Is the tape library equipped to minimize the extent of fire damage?

4. Fire Alarms

- Have appropriate fire detection and alarm systems been installed in the computer room?
- Are the locks on the computer room doors released when the alarm sounds?
- Has appropriate fire detection system been installed in magnetic media storage libraries?
- Are closets and unused areas equipped with detection and alarm systems?
- Are fire detection and alarm systems monitored around the clock? Where? By whom?
- Are tile lifters available in raised floor areas, to enable tile removal for the investigation of alarm conditions and fire suppression?

5. Fire Suppression Systems

- Is the building equipped with an automated fire suppression system?
- Is the computer room equipped with an automated fire suppression system?
- Where halon is being used, are abort buttons located near exit doors in the computer room?
- Are hand-held fire extinguishers of appropriate type and charge mounted near exit doors in the computer room? Are employees familiar with use?
- Is an automatic fire suppression system installed in the magnetic media library?
- Are hand-held fire extinguishers of appropriate type and charge mounted near the library exit doors? Are employees familiar with use?
- Have the automatic suppression systems installed in all critical areas been inspected and tested recently?
- Have all fire extinguishers been tested recently/on a regular basis?

6. Storage of Combustible Materials

Is the storage of the following combustible materials prohibited in the computer room and in the magnetic media library:

- Blank paper stock (other than small quantities required for one day's production)?
- Cleaning compounds/ materials?
- Oils or fuels?
- Are printed materials and garbage removed from the computer room on a regular basis?
- Are combustible materials stored in areas not suited for this function?

7. Administration

Are fire and emergency procedures defined for employees to follow, and are they tested on a regular basis, to ensure that:

- Power to the machine room is shut down in the appropriate sequence?
- The magnetic media storage vault/ safe is closed
- Evacuation is made in a timely manner?
- The fire department is notified?
- Has the local fire department reviewed the fire detection and suppression systems, as well as the emergency evacuation procedures?
- Are the areas under raised floors cleaned regularly?
- Is smoking prohibited in the following critical areas?
  - Computer room
  - Magnetic media storage library
  - Data processing supply rooms
  - Vendor storage rooms.

E. WATER PROTECTION

Control Objective

- To ensure that electronic processing equipment and critical resources are adequately protected against the threat from water damage.

- Is the data centre facility located in an area, which might be subject to flood?
- Has the potential for water damage from seepage (floors or roof above) been minimized? Are waterproof covers available to protect equipment from falling water?
- Review types/ sources of water supply.
- If water pipes extend above the room, or a wet sprinkler system is installed, are waterproof covers or water deflectors available/ installed to protect equipment? What is activation method for water pipes? Dry charge system used?
- Are water detection and alarm systems installed under the raised computer room floors and in magnetic media storage libraries?
- Are water detection alarms monitored around the clock?
- Are computer rooms and magnetic media library floors drained and/ or are pumps available to remove water?

F. OTHER HAZARDS

Control Objective

- To ensure that the facility is adequately protected against hazards other than fire and water.
- Where the processing facility is located in an area with a history of:
  - Severe snow storms
  - Tornadoes
  - Hurricanes
  - Flooding
  - Earthquakes
  - Lightning
  - Riots, civil disorders, union strike activities
  - High crime/ theft levels
  - Arson; or
  - Other potential disasters.

- Has appropriate physical protection been implemented to minimize the potential for damage?

- Are critical resources (i.e., PCs, expensive equipment) protected from theft and/or destruction? Are they locked, bolted or chained down?
- Is there a procedure in place for checking out equipment leaving the building?
- Is there an active asset management program in effect? Are inventory lists maintained? By whom? Are equipment locations tracked? How often are inventories conducted?
- Are general supply/equipment storage areas protected? Are there dock/receiving area procedures for temporary storage of incoming supplies and equipment?
- Are supply quantities limited as much as possible? What is current re-supply time frame (e.g., 30 days)?
- General housekeeping condition? Storage hazards?
- Are stairwells, elevators, and exit doors, other public access areas clear of hazards?
- Are surveillance cameras (CCTV) used? If so, what areas are covered (interior/exterior)? Who monitors? From which location? What reports are filed? With whom? Video taping? How long are tapes retained?
- Are shredders or other means available for the destruction of confidential or sensitive documents? Are employees aware?
- Are all departments involved in the threat assessment process?

G. ELECTRICAL POWER

Control Objective

- To ensure that the electrical power supply to the computer room, printing, and operations areas (in which processing equipment are located) is reliable and adequately safeguarded.
- Does the facility have a history of power fluctuations, brownouts, or total power loss?
- Are power fluctuations monitored and recorded?
- Has a power filtering system been installed? Are surge protectors in use?

- Is an uninterruptible power supply (UPS) installed ... and is it capable of maintaining desired service?
- Is a power back-up generator available with an adequate supply of fuel?
- Are the UPS and back-up generator tested on a regular basis and for a reasonable length of time?
- What is the condition/ arrangement of electrical cords, wiring?
- Are there separate power feeds into the building? From separate generating station sources? Different power grids? Or is there a single point of failure with respect to incoming power?
- Is the emergency power supply capable of maintaining all equipment, including all electronic access control devices and telephone services?
- Is the UPS fitted with an alarm, which is monitored around the clock?
- Is the power source for the computer room independent of that for the rest of the facility?
- Is access to the building's power source adequately controlled?
- Is access to power control panels, junctions, and cabling restricted?
- Is there an emergency power off (EPO) switch located at the computer room exits?
- Is emergency lighting installed and in operating order?
- Are exit lights clearly visible?
- Are operations staffs trained in emergency response procedures dealing with electrical power hazards?
- Are there procedures, which will enable operators to affect an orderly and efficient recovery following a power failure?

H. ENVIRONMENTAL CONTROL SYSTEMS

Control Objective

- To ensure that the computer room and other processing areas have adequate environmental control and monitoring systems in place.
- Are monitoring, regulating, and alerting systems installed for:

  - Humidity?
  - Temperature?
  - Airflow?
  - Dust?
- Are monitoring and alerting systems checked around the clock?
- Are there provisions for back-up air conditioning?
- Are there provisions for a back-up water supply for the air conditioning?
- Have other appropriate measures been taken to combat static electricity?
- Are food and drinks prohibited from all secure areas?
- What is the policy on smoking in the building?

I. ENTRY PROTECTION

Control Objective

- To ensure that entry to the facility, which houses the computer room and other, critical processing resources is adequately controlled to prevent unauthorized persons from gaining access. In addition, to ensure that the entry points for external communication and utility services are adequately secured/ protected.

1. Building

- Is the building located in an area subject to break-ins, arson, and high crime? Has client checked with local police or sheriff's office?
- Is the company the sole occupant of the building, or is there a potential threat posed by other tenants?
- Who are the neighbours? Any businesses, which might be targets for terrorists, arsonists, burglars?
- Is the perimeter area adequately secured and monitored?
- Is there access into the building from any level other than the ground level? Second floor? Roof entrance?
- Are employees required to wear identification (ID) badges at all times?

- Do ID badges bear a photograph of the owner and indicate area(s) of access?
- Is the issuance of ID badges authorized and subject to strict control?
- Are card, key, and/ or combination access devices used? How are they controlled?
- Are building visitors escorted when on the premises?
- Are lists/ rosters of authorized personnel (by facility area) maintained, posted, and updated on a regular schedule? Who approves? Who re-certifies? Are procedures documented?
- Are access control lists used for special or restricted areas? Who approves/ re-certifies? How often? Are procedures documented?
- Is all entry to and exit from the building outside of regular hours monitored and logged?
- Is prior approval of off-hour entry by employees required?
- Are all other building entry points secured (garages, emergency exits, delivery entrances, air intakes, mail slots, etc.)?
- Are all exterior doors and windows equipped with intrusive alarms, which are monitored and tested regularly?
- Is there a Building Directory, which shows the location of the computer room (or other sensitive areas)?
- Are data processing/ computer room areas unmarked for deliveries, parking, etc.?
- Are building utility rooms, which provide primary sources of electrical power and communication lines (telephone and wiring/utility closets, riser rooms) unmarked and secured?
- If applicable, what are access issues related to other building tenants?
- Are the following adequately protected?
  - Cooling towers?
  - Water supply?
  - Air conditioning?
  - Heating systems?

2. Computer Room

- Is employee access to/from the computer room controlled and logged?
- Is the computer room physically separated from the other areas of the data centre facility by walls, which extend from concrete slab to slab?
- Is access to the computer room restricted to authorized operations personnel only?
- What is the policy on computer room access by vendors/suppliers and other non-employees?
- Are the doors to the computer room kept locked at all times?
- Are the doors hung in such a way as to prevent hinge pins from being removed from the outside?
- Are all computer room entrances fitted with alarms, which are appropriately monitored?
- Are doors fitted with electronic entry control devices, combination locks, or mechanical key locks?
- Where combination locks are in use, are combinations changed regularly, and the distribution of new combinations adequately recorded and controlled?
- Where card entry devices are used, is the issue of cards subject to appropriate authorization and control?
- Where doors are fitted with mechanical door locks, is the issue of keys subject to appropriate authorization and control?
- Is an up-to-date key, combination, or card holder master list maintained?
- Do the entry control systems automatically record computer room entry/ exit?

3. Magnetic Media Storage Areas

- Are the magnetic media storage areas physically separated from other areas by walls, which extend from concrete slab to slab?
- Is entry limited to authorized librarians and is the library kept locked when an authorized librarian is not present?
- Are the doors hung in such a way as to prevent hinge pins from being removed from the outside?
- Are all library entrances and windows fitted with alarm systems, which are monitored appropriately?
- Are entry doors to the library fitted with electronic card devices, combination or mechanical key locks?
- Where combination locks are used, are combinations changed regularly, and is the distribution of new combinations adequately recorded and controlled?
- Where card entry devices are used, is the issue of cards subject to appropriate authorization and control?
- Where doors are fitted with mechanical key locks, is the issue of keys subject to appropriate authorization and control?
- Is an up-to-date key, card, or combination holders' master list maintained?
- Where the library is equipped with a vault for the storage of the most critical files, is the vault kept locked when not in use/ accessed?
- Is the combination on the vault changed regularly and subject to appropriate control?

4. Visitor Security Procedures

- Are colour coded visitor badges used and displayed at all times?
- Do the guards or receptionist require advance authorization and/ or positive identification of all visitors before badges are issued?
- Are visitors required to be escorted at all times?
- What is the policy covering "regular" (as opposed to one-time) visitors and on site vendors?
- Are Data Processing personnel trained to challenge unaccompanied visitors and strangers in restricted areas, and to advise building security when a challenge has been ignored?
- Is a visitor "sign in/ sign out" log maintained? Does it list information such as visitor name, where he/ she is visiting, who is escorting the visitor and temporary badge number assigned?
- Are the visitor logs reviewed by management on a regular basis?

- Are there procedures listing which areas visitors are not permitted to enter?

5. Maintenance and Janitorial Personnel

- Are janitorial, equipment, and utility service personnel subject to the same screening, logging, and escort requirements as other computer room visitors?
- Do they have access to sensitive or confidential information/ documents (trash)? Disposal methods? Are shredders used (for sensitive/ confidential document destruction)?
- Are shredders used to destroy confidential or sensitive information/ documents, which are destined for trash, pick up?
- Are there procedures covering what they can/ cannot handle? Areas, which are off limits?

6. Vendors

- What agreements are in effect re: vendor access within the building? Are procedures documented?
- Are separate areas/ storage rooms maintained within the facility for use by vendors? If so, what controls are in place?

J. OFF-PREMISE STORAGE FACILITIES

Control Objective

- To ensure that adequate security is enforced over the physical movement of magnetic media and that off-site media storage is adequately protected, both physically and environmentally.

1. Movement of Magnetic Media

- Is **magnetic media secured** and appropriately controlled during transportation?

2. Access to the Off-Premises Storage Facilities

- Is the off-site storage facility kept locked at all times when not being accessed to store or retrieve backup?

- Are the doors to the facility hung in such a way as to prevent hinge pins being removed from outside?
- Are external windows on the facility reinforced and barred?
- Are doors and windows fitted with alarms connected to the local police department or alarm monitoring company?
- Where a key lock is used on the doors, is the issue of keys under appropriate control and is a master listing of key holders maintained?
- Where a combination lock is used, are combinations changed regularly and is the issue of combinations suitably controlled?

3. Fire Protection

- Are facility walls, floors, and ceilings constructed of fire resistant materials and constructed to industry standards (e.g. NFPA)?
- Are adjacent areas free of highly flammable materials?
- Are external building air/heat ducts, which enter the facility, lined with non-combustible material and equipped with power dampers to prevent smoke migration?
- Is the storage of combustible materials in this facility prohibited?
- Are automatic heat and smoke detection systems installed and monitored around the clock?
- Are automatic fire suppression systems of an appropriate type installed?
- Are hand-held extinguishers of an appropriate type and charge mounted near the facility?

4. Water Protection

- Is the facility located in an area that may be subject to flood?
- Are waterproof covers available to cover magnetic media?
- Are water intrusion alarms fitted and monitored around the clock?
- Are facility floors drained to remove excess water?

5. Other Hazards

- Are temperature and humidity ranges experienced in the facility within tolerance?
- Is the facility located in an area with a history of:
  - Severe snow damage?
  - Tornadoes/ hurricanes?
  - Earthquakes?
  - Lightning?
  - Riots?
  - Other potential disasters?

- If off-site storage facilities are contracted, are there written procedures for the retrieval of magnetic media?
- Have retrieval procedures and authorized personnel been agreed and identified with the third party service?

K. PHYSICAL SECURITY OF DOCUMENTATION

Control Objective

- To ensure that hard copy system, program, operations and user documentation are securely stored and restricted to authorized personnel.
- Is a master copy of hard copy documentation catalogued and indexed?
- Is the master copy appropriately secured both during and after hours?
- Is one person designated as documentation librarian, whose function (defined in writing and supported by written procedures) is to maintain custody over the documentation?
- Is the facility/ container in which the documentation is stored constructed of fire resistant materials (with at least a one hour rating)?
- Is a backup copy of master documentation maintained in a secure off-site location?
- Are there procedures to ensure that all changes to the master copies are reflected in the off-site backup copies?

L. PHYSICAL PROTECTION OF COMMUNICATION EQUIPMENT

Control Objective

- To ensure that host communication equipment, and computer and communications equipment located outside of the computer room is adequately protected against theft, destruction and unauthorized use.

1. Host Communications Equipment

- Is there a central Network Operations Control Centre (NOCC) associated with the host or mainframe system(s)?
- Is access to this area restricted to designated communications or DP department personnel?
- If modems and communication controllers are not in the computer room, is access to them effectively restricted?
- Are all communication line termination panels secured?
- Is emergency power for communications equipment available and secure?

2. Remote Communication Equipment

- Are all communication line termination panels secured?
- Is emergency power for communications equipment available and secure?
- Are modems, communication controllers, visual display terminals and other equipment:
  - kept in a physically secure environment separate from the general office areas?
  - supervised by authorized staff during office hours?
  - secured from general access after hours?
  - equipped with physical key locks for which the keys are removed and secured outside of regular office hours?
- Is suitable fire detection and suppression available to protect the communications equipment?
- Is communication equipment in remote locations located in areas that may be subject to flood?

- Has the potential for water damage from sprinklers or floors above the area, been minimized?
- Given the location of the remote communications equipment, have adequate measures been taken to minimize the potential for damage from other hazards?

Annexure 2

Sample Checklist for Application Controls

Background Information

A. Technical/ Information Systems

1. Determine what hardware is used to run the system. Classify the system as micro, LAN, client/ server or mainframe based.
2. Determine if the software was purchased or developed in-house.
3. If the software was purchased, determine if any vendor warranties are still in force. Also determine if the vendor is financially sound and if the software is held in escrow.
4. If the software was developed in-house, verify that the software was developed and updated based on a sound systems development methodology.
5. Identify the programming languages used in the application. Determine if the Information Systems Department has programming staff knowledgeable in these programming languages.

6. Identify the types of data files used in processing (data base, sequential files, disk, and tape).
7. Identify the primary transaction, master and reference files used in processing.
8. Determine how Information Systems controls and secures access to the application programs.
9. Determine if passwords are entered in such a way that they are not displayed.
10. Evaluate the quality of the programmer application documentation (should include system and program flowcharts, decision tables, file layouts, data element definitions, narratives, source program listings, record of changes).
11. Evaluate the quality of the application operations documentation (should include job and system flowcharts, input and output descriptions, job frequency and sequence of operation, job restart/ recovery procedures, file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, data capture instructions).
12. Determine if backup copies of application program and operations documentation are stored off-site.
13. Determine if Information Systems monitors processing flows to verify application programs run according to schedule.
14. Business rules to be mapped to the application.
15. User specifications decided and agreed upon by the management.

B. End-Users

1. Determine the primary means of data entry and processing (batch, on-line, real time).
2. Determine if the organization practices data ownership. If so, identify and interview the data owners to determine if they understand their roles and responsibilities.
3. Interview a sample of end-user managers to determine end-user management attitudes regarding the quality and effectiveness of the system.

4. Determine from end-user management what they perceive to be the risks, exposures and limitations associated with the system.
5. Determine the number of end-users working with the system, their locations and responsibilities associated with the system. Obtain an organization chart for these positions and people.
6. Determine if this application generates data for legal or regulatory agencies. (If so, pay extra attention to these transactions).
7. Evaluate the quality of end-user documentation (Should include description of the system, description of source documents and procedures for their preparation, job submission procedures, control procedures, error identification and correction procedures, description of output reports and their use).
8. Identify the application training available for end-users. Evaluate this training to determine if it is adequate, current and available for new people.
9. Determine if end-user activity is adequately supervised.

C. System Interfaces

1. Determine what other applications interface (manually or electronically) with this application. Document what is received from and what is sent to these other applications.
2. Determine how end-users verify or establish assurances that interfaces are providing complete, accurate and authorized data.

D. File Handling

1. Determine the retention periods for the various key application data files. Evaluate if the retention periods satisfy management reporting, IRS reporting and internal accounting requirements.

2. Determine if end-user management and data owners are aware of the retention periods of the various key application data files, and if these managers are satisfied with the length of retention.

E. Backup and Recovery

1. Determine how often key files are backed up. Determine if copies of these backup files are stored at a suitable off-site facility
2. Verify that the off-site backup file storage facilities are secure.
3. Determine if application recovery plans exist (both technical and end-user) for restoring from short-term and long-term interruption of computer processing. Verify that these plans address both technical restoration needs and alternative end-user processing procedures.
4. Determine if these application recovery plans have been tested in the last year.
5. Establish how long the organization could comfortably function and avoid significant financial loss if the computerized aspects of this application failed. Verify that restart/recovery and disaster recovery plans provide for restoring this application in the time needed to avoid significant financial loss.
6. Determine if Information Systems has established data file and record retention periods. Determine if these retention periods are reasonable for backup, disaster/ recovery and audit purposes.
7. Verify that restart/ recovery plans from short-term computer interruptions include the ability to identify the status of all processing to the point of application failure to establish a cut-off for transaction re-entry.

F. Identify all Subsystems

G. Identify all transactions within each subsystem (including those automatically generated by the computer).

H. For each transaction, use Schedule-1, Transaction Worksheet, to record and evaluate application controls and procedures.

Annexure 3

Application Controls Audit

SCHEDULE I

Transaction Worksheet

System: ____________________

Subsystem: ____________________

Transaction: ____________________

A. Input Controls

Input controls ensure transactions are:

- Input into and accepted by the computer,
- processed only once,
- with no duplicates, and
- errors in financial and non-financial data fields are:
  - identified
  - segregated from valid transactions
  - corrected in a timely manner, and
  - returned to mainstream processing.

1. How does the transaction originate?
2. How is the transaction authorized (manual signature, electronic signature, screen access authorization, etc.)?
3. Who inputs the source data? Are these people separate from those who reconcile the results of processing?
4. How is the source data input into the application (batch, on-line)?
5. Determine if there is automatically triggered processing that will change the application data. If yes, determine how updates of these kinds are authorized, identified and reconciled. Determine what controls are in place to ensure the accuracy of the events that trigger the automatic processing (date, inventory re-order point, etc.).
6. Is data entry conducted within a short time after the source document is created?
7. After source documents are entered into the application, are they check marked or signed in some way to indicate that they were entered, reducing the risk of accidental duplication or reuse of the document?
8. Is there an appropriate separation of duties (custody, authorization, recording, and periodic Reconciliation) for those authorized to update data?
9. How are source data documents controlled for completeness and accuracy (pre-printed turnaround document, sequentially pre-numbered, securely stored after being authorized, tagged after input)?
10. Is there a retention period for source data?
11. Identify the controls in place to ensure completeness and accuracy of input (reconciliation of control totals, 1-for-1 checking, matching, sequence checking, duplicate processing, and programmed edit checks).
12. Determine if and how the following automated edit checks are performed on the input data:
    a. Reasonableness
    b. Dependency

c. Range
d. Existence
e. Format
f. Check digit
g. Prior data matching
h. Consistency
i. Others.

13. If appropriate, do the following edit checks exist:

- Format checks on numeric data
- Range checks on variable numeric field
- Date tests on date fields
- Existence checks on all key fields
- Check digits on all identification keys
- Tests for missing data
- Tests for extraneous data
- Tests for record mismatches
- Tests for out of sequence conditions.

14. If input controls include use of control totals, are the computer-generated totals being compared to independently established totals?
15. What reports do users get to verify and monitor the operation of the application (controls totals, summaries, error counts, exception reports, etc.)?
16. How do supervisors or managers verify the production control totals checking procedures are being performed?
17. Describe any comparisons of results of runs to previous runs for reasonableness checks.
18. How do the users verify updates to the files against authorizations?
19. Determine how duplicate transactions are prevented or identified.
20. Determine if and how data received from other applications is validated for completeness and accuracy.

B. Processing Controls

Processing controls insure transactions are:

- accepted by the computer
- processed with valid logic
- Carried through all phases of processing and
- updated to the correct data files.

1. Are users required to provide processing parameters and, if so, how are they authorized and verified?
2. Identify the controls in place to ensure completeness and accuracy of processing (run-to-run control totals, duplicate processing, etc.).
3. Document the end-user reconciliation procedures that facilitate completeness and accuracy of processing.
4. What reports do users get to verify and monitor the operation of the application (controls totals, summaries, error counts, exception reports, etc.)?
5. Describe how user office personnel check the production control totals.
6. How do supervisors or managers verify the production control totals checking procedures are being performed?
7. Describe any comparisons of results of runs to previous runs for reasonableness checks.
8. How do the users verify updates to the files against authorizations?
9. Determine if special reconciliation procedures need to be applied to month-end, fiscal year, etc. cut-off.

C. Error Correction

10. Identify all data and processing errors that can be identified, either through edits or routine processing.
11. Determine the impact data and processing errors have on processing (errors must be corrected before processing continues; errors are segregated from processing so good transactions may continue to be processed while errors are

corrected).

12. Determine if errors are segregated onto a suspense file. Determine if the error suspense file is cumulative or non-cumulative.
13. Review the error reports to determine if they are of reasonable length.
14. Determine how errors are corrected.
15. Determine if the corrected transactions are authorized.
16. Verify that the corrected transactions are reintroduced into mainstream processing either at the original point of input or through a special error correction process.
17. Determine if the error correction process removes the items from the error suspense file.
18. Determine the timeliness of error correction.
19. Identify how end-users monitor the remaining errors and conduct timely further investigations.
20. Is there an appropriate separation of duties (custody, authorization, recording, and periodic reconciliation) for those authorized to update data?
21. Determine if all reconciliation and error correction procedures are documented in the end-user documentation.
22. Is an exception report generated for long-outstanding error transactions, with an aging analysis?

D. Output Controls

Output controls ensure output data is:

- reported in the correct manner,
- viewable/ available to only authorized personnel,
- appropriately retained or destroyed,
- subject to necessary processing audit trails, and
- If erroneous, segregated from valid transactions, corrected, and re-entered into mainstream processing.

1. Identify how output is distributed. Determine if this distribution reduces exposes to unauthorized viewing of sensitive information by either involving remote printers at end-user locations or use of output distribution checklists.

2. How does the organization ensure that reports and files are distributed to the correct end-users (report routing, remote printers)?
3. Who receives the output reports? Are they separate from those conducting input?
4. How does the end-user verify that all reports were received and that all pages of the reports were included (standard report titles, page numbering (1 of ?), and end-of-report indicator)?
5. Do output reports include the following identifying information:
   - Report title.
   - Processing program name/number.
   - Date and time report was produced.
   - Processing period covered.

6. How does the end-user evidence receipt of reports and files (check lists, sign-off, etc.)?
7. Is there an appropriate separation of duties (custody, authorization, recording, and periodic reconciliation) for those authorized to update data?
8. How are confidential reports identified and distributed?
9. Identify all special forms used in processing and reporting. Determine if sensitive forms are secured (stored in secured areas, laser printed forms, etc.) and accounted for (pre-printed and sequentially pre-numbered forms, multi-part forms, laser printed forms, etc.).
10. Are the people responsible for securing sensitive documents different from those who maintain the related accounting records?
11. Are there special disposal procedures for sensitive reports (shredding, special secured filing)?

E. End-Documentation

User documentation is the primary source of information for all personnel responsible for day-to-day use of the application.

1. Does end-user documentation exist explaining proper source document origination, authorization, data collection, input preparation, report handling, error correction and report/data retention?
2. Are source documents retained so that data lost or destroyed during subsequent processing can be recreated?
3. Does each type of source document have a specific retention period?

F. Authorization

Authorization controls ensure all information and data entered or used in processing is:

- authorized by management, and
- Representative of events that actually occurred.

1. If transactions are manually authorized, what controls ensure that no unauthorized modifications take place after authorization, but prior to establishing input controls? Determine if the proper level of management is authorizing the transaction activity.
2. If transaction authorization is facilitated by logical access restrictions, select a sample of access rules applying to transaction input and update, and verify the appropriate people have these capabilities.
3. Identify any allowable overrides or bypasses of data validation and edit checks (authorization, monitoring, etc.). Determine who can do the overrides and verify that they are in a management position that should have this authority. Are all uses of the override features automatically logged so these actions can be subsequently analysed for appropriateness?

G. Security

Security controls ensure access to information and facilities are restricted to only those individuals designated by responsible management.

1. Identify the primary transaction, master and reference files used in processing. Work with Security Administrators to determine if these files are secured from unauthorized access.
2. Evaluate how security access restrictions are maintained. Items of importance include security administration, logon/ password management, and security monitoring and data ownership.
3. Evaluate methods for restricting access to source documents and blank input forms to only authorized personnel only.
4. Determine if data entry terminals are located in secured locations.
5. Determine if remote printers are located in secure locations that protect against unauthorized access.

H. Separation of Duties

1. Are duties separated such that no one individual performs more than one of the following operations?

- Transaction authorization
- Transaction originating
- Transaction input
- Distributing output.

2. Are rejected transactions not caused by entry errors corrected by the user originating the transaction?
3. Does the end-user have ultimate responsibility for the completeness and accuracy of all application data?

I. File Maintenance

Maintenance controls ensure data stored on computers is kept current and up-to-date, and that unusual data requiring action or change is identified. This applies particularly to reference and standing data files.

1. Identify all reference and master files used in this application.
2. Identify file update notification procedures applied to these files (turn around documents, electronic mail notices, control totals, etc.). Determine if end-users use these update notification procedures to verify the updates to these files.
3. Determine if these files are reviewed on a regular basis to verify if the contents are current and up-to-date.

RBI Checklists for Computer Audit

CHECKLISTS FOR COMPUTER AUDIT

Contents

Questionnaires

Chapter 1

Introduction

1.1 The Jilani Working Group on internal controls and inspection/ audit systems in banks (1995) Identified key risks associated with IT systems and recommended various control measures to address these risks. It recognized the need for a specialized system of EDP audit and recommended that the entire domain of EDP activities should be brought under the scrutiny of the Inspection and Audit department. Banks were advised by the Department of Banking Supervision (DBS) of the Bank to expeditiously implement the recommendations of the group.

1.2 The risks and controls systems in computerized banks were analysed by Coopers and Lybrand (UK) under the Technical Assistance Project funded by the Department for International Development (DFID) UK. Based on the consultancy report, DBS had issued in1998 a detailed guidance note to banks apprising them of the risks in computerized environment and suggested associated

controls to address the specific risk. An inspection manual was also prepared in 1997 with the assistance of the aforesaid international consultants for the guidance of the Reserve Bank officers inspecting banks with computerized accounting system. An assessment of the system of EDP audit in the concerned bank is now an integral part of the Annual Financial Inspection of banks.

1.3 An assessment of the system of computer audit in banks as on March 31, 2000 was made based on the basis of findings contained in the inspection reports of banks for the year 1998-99 and 1999-2000 and other specific feedback received from banks. Structured questionnaires were sent to all the banks eliciting information on the nature of the Information Technology (IT) management function, IT risk management and EDP audit systems, EDP audit methodology etc. The analysis revealed that the system of computer audit in banks is still in the developmental stage. A range of policy approaches has been reported in regard to the conduct of EDP audit by banks. It was observed that in respect of 50 percent of banks, the policy on IT risk management and EDP audit were not duly documented. In respect of many banks even availability of EDP inspection manuals was not ensured. The periodicity for conducting such audits also was not uniform across banks. The practice in most of the banks in India was to audit around the computer. Computer security issues did not receive adequate Top Management attention. It was evident from the assessment that the computer audit in India had been still evolving and a major constraint encountered by banks is the general shortage of skilled technical personnel for the task. The findings of the assessment were put up to the Audit Sub-committee of the Board for Financial Supervision as per the Board's direction.

1.4 The Audit Sub-committee decided that a small committee comprising representatives of RBI, ICAI, SBI, a foreign bank and a new private sector bank may be constituted to draw upon a check list in a standardised form so that all the banks operating in the country can ensure that their computerized branches are applying requisite controls in the computerized environment and the branch auditors also verify the same and report accordingly. Accordingly, a committee was constituted with Shri A. L. Narasimhan, Chief General Manager-in-Charge, Department of Banking Supervision, Central Office as the Convener.

The Composition of this Committee is as follows:

1. **Shri A. L. Narasimhan -** Convener
   Chief General Manager-in-Charge
   Department of Banking Supervision, CO
   Mumbai - 400 005

2. **Shri Ashok Kumar Chandak/ Shri R. Bupathy**[1] - Member
   Vice President
   The Institute of Chartered Accountants of India
   Indraprastha Marg
   New Delhi - 110 002

3. **Shri S. Santhanakrishnan**
   Chairman, Committee on Information Technology
   The Institute of Chartered Accountants of India
   Indraprastha Marg
   New Delhi - 110 002

4. **Shri S. N. Pattnaik** - Member
   General Manager
   State Bank of India
   Inspection Department
   Corporate Centre
   Hyderabad

5. **Shri Atilla Karasappan** - Member
   Vice President, Senior Country Operations Officer
   Citi Bank,
   5th Floor, Plot C-61, B-K Complex
   G-Block, Bandra (E)
   Mumbai - 400 051

6. **Shri Ashok Kumar Patni** - Member
   Executive Vice President & Head - Audit
   Methods & Inspection Department
   ICICI Bank Ltd, ICICI Towers
   Bandra Kurla Complex
   Mumbai - 400 051

7. **Shri R. Ravikumar** - Member Secretary
   Assistant General Manager, Reserve Bank of India
   Department of Banking Supervision
   Central Office
   Mumbai - 400 005

The terms of reference of this Committee was:
To draw upon a check list in a standardised form to conduct computer audit so that all the banks operating in the country can ensure that their computerized branches are applying requisite controls in the computerized environment and the branch auditors also verify the same and report accordingly.

1.5 The Committee had its first meeting on 1st November, 2001. The levels of computerization of banking industry, earlier work done in this regard and guidelines already issued by DBOD/ DBS in this connection were discussed in detail. Different levels of

[1] **Shri Ashok Chandak** was the Vice-President of ICAI when the Committee was formed. **Shri R.Bupathy** substituted him as the member in the Committee consequent on his election as the new Vice-President.

computerization of different banks, availability of different platforms in different banks etc. were discussed and it was decided to prepare a standardised checklist for conducting computer audit.

It was felt by the committee that IS Audit Checklist prepared need to be platform independent and necessary platform dependent control questionnaire can be framed by the banks themselves. Computer Audit questionnaire also should be bank independent. On the basis of the practices followed by individual banks they may frame bank specific control questionnaire.

1.6 The committee decided to classify the areas of risk in the IS environment as under:

1. Business Strategy
2. Long Term IT Strategy
3. Short Range IT Plans
4. IS Security Policy
5. Implementation of Security Policy
6. IS Audit Guidelines
7. Acquisition and Implementation of Packaged Software
8. Development of software - in-house and outsourced
9. Physical Access Controls
10. Operating System Controls
11. Application Systems Controls
12. Database controls
13. Network Management
14. Maintenance
15. Internet Banking.

1.7 These areas were allotted to members of the committee to prepare relevant checklist for the respective risk areas. The checklist thus prepared was discussed by the committee in its subsequent sittings. On the basis of the deliberations a draft report was prepared and circulated to all the members for their comments. On receiving comments from the members, the checklists have been finalized and presented in the report.

Scheme of the Report

1.8 This chapter records the background for the constituting the Committee; the terms of reference and summary of recommendations of the Committee. In the next chapter, levels of computerization of banking industry, earlier work done in this regard and guidelines already issued by DBOD/DBS in this connection, different levels of computerization in banks etc. are discussed along with possible benefits of the checklists. The checklists in respect of the 15 areas of audit interest indicated in the above paragraph have been included as separate chapters in the report.

1.9 Acknowledgements

The committee places on record its gratitude to the Audi Sub-committee for constituting the committee on computer audit. The convener acknowledges the co-operation extended by all the members of the committee in completing the task entrusted and making the discussions meaningful. The keen interest shown by all the members of the committee in preparing the checklists for computer audit is appreciable. The committee acknowledges with thanks the RBI, ICAI and commercial banks for nominating senior officials for the committee and making their valuable time available. The committee further acknowledges the significant contributions made by officials of RBI, ICAI and commercial banks, who were not members but contributed in building up the checklists. Notable contributions were made by Shri R. Suriyanarayanan, ICAI, Shri Vikram Subrahmanyam and Shri Ramesh Lakshminarayanan from Citi Bank, Shri Gokul Chander from ICICI Bank, and Shri P. Parthasarathi, DGM from RBI. The committee received significant contributions from Shri. R. Ravikumar as the Member Secretary.

Committee acknowledges his dedication with gratitude and likes to record its appreciation for his outstanding work. The committee acknowledges the services of Shri M. K. Prabhu, Assistant Manager and Shri P. B. Uday in making arrangements for the meetings.

1.10 Summary of Recommendations

The basic purpose for preparing checklists for conducting computer audit is to sensitise banks on the emerging concerns arising on account of computerization and growing dependency on computers and technology for conducting the business. It is expected that these checklists would bring about a minimum standard in conducting the computer audit. The checklists may be used by all the commercial banks as general guidelines for conducting computer audit. These may be circulated to appropriate levels of management so that the computer audit practices followed by banks are at least of a minimum standard. However, those banks which are following much more exhaustive checklists for conducting IS Audit/ Computer Audit may continue to do so.

Recommendations

- The checklists for conducting computer audit in commercial banks and financial institutions may be circulated to all commercial banks and financial institutions under the supervisory jurisdiction of RBI.
- Banks and FIs may be advised to follow the checklists as general guidelines and those banks/ institutions which are following better practices may continue to do so.
- The checklists may be circulated to all the Regional Offices of DBS so as to enable the inspecting officers to conduct the computer audit at the time of financial audit. Suitable extension of time may be given to the inspecting officials.
- A copy may be forwarded to Inspection Department of the Bank, who are responsible for conducting internal audit of RBI for their use.
- Periodical training/ seminar on this area may be conducted at RBSC (for inspecting officials of RBI) and BTC (for commercial banks) on a continuous basis.
- A cell may be formed at Central Office of DBS, which will scrutinize the reports prepared by the inspecting officials so that necessary corrective action may be suggested to banks through BMDs or CPOSs as the case may be. Further this cell may continue to update the checklists with latest developments and concerns so that the checklists remain current and relevant.

A. L. Narasimhan
Convener, RBI

R. Bupathy
Member, ICAI

S. Santhana Krishanan
Member, ICAI

S. N. Patnaik
Member, SBI

Atilla Karasappan
Member, Citibank

Ashok Kumar
Member, ICICI Bank

Patni R. Ravikumar
Member - Secretary, RBI

Mumbai
April 2, 2002

Chapter 2

Standardised Checklist for Conducting Computer Audit

2.1 Banking business is different from other businesses in many ways with the single important difference being banks are the custodians of the public money. Banks are intermediaries facilitating mobilization of deposits from savers and lending the same and in the process earn a reasonable spread so that they can meet the expenses involved in carrying out the intermediary business and generate adequate return for the capital providers. Banking system plays a very important role in the economic development of the country and hence always been subjected to severe controls as compared to any other industry.

2.2 Until recently, banking transactions were put through manually. However, the banking world has changed dramatically in the past ten years and thanks to the technological developments the level of computerization in banking industry has gone up manifold. Computers are extensively used to process data and to

generate Management Information now. As the technology is becoming affordable, more and more players are adopting the high level of computerization for carrying out the business. Information technology is at the centre of strategic business management, delivering value to customers, fostering customer centric culture, exploring the internet channel, information and knowledge assimilation, risk mitigation and management, these elements being critical success factors in emerging markets.

2.3 We are aware of the benefits of adopting new technologies and computerization to the shareholders, management and customers. But it needs to be understood that technology changes the business processes and we are embarking on an un-chartered territory as far as controls are concerned. As Central Vigilance Commissioner said, technology is in a way like Lord Vishnu, who is described as "bhaya krita bhaya nashana". He is both the 'creator of fear and also destroyer of fear'. So if technology can lead to frauds, it can also devise systems to check the fraud.

2.4 “Knowledge is of two kinds. We know of a subject ourselves or we know where we can find information upon it Samuel Johnson. This quotation is appropriate for Information Technology. Even if one does not know the subject, there are many information providers. On the issue of information technology in the banking industry a lot of pioneering work has already been done. Some of the work relating to this area by RBI is indicated under:

1. Jilani Committee Recommendations: It was recommended that the Information System audit needs to be brought under Inspection Departments of Banks

2. Narasimham Committee Second: The committee reiterated the importance of IS Audit in Banks

3. Vasudevan Committee: The committee has underlined the importance of computerization and computer resources and suggested ways to embrace it.

4. Internet Banking Committee: The report prepared by a group on behalf of RBI, has highlighted several important security issues in Internet Banking and has recommended IS Audit.

5. Working Group for Information System Security for the Banking and Financial Sector headed by Dr. R.B.Burman, E.D: The working group has prepared a document on Information System Audit Policy and the same has been circulated among all banks by the Department of Information Technology, RBI recently. Though the document has been forwarded to IBA for necessary action, this would serve as a basic document for bank on IS Audit and IS security issues.

2.5 Instructions / Guidelines Issued by DBS / DBOD

1. Inspection Manual for Banks with Computerised Accounting Systems document prepared with the help of Coopers & Lybrand (UK C&L) for internal circulation among RBI Inspectors.
2. Guidance Note on Record Maintenance January 1998.
3. Guidance note for Banks on Risks and Controls in Computer and Telecommunication Systems.
4. DBOD circular on Internet Banking.
5. DBS circular on EDP Audit cell to be part of Inspection & Audit Department in Banks dated June 1999.

2.6 The Current Work

Audit Sub Committee of the Board for Financial Supervision, while discussing the level of computerization in banks and the control over the same desired that a committee may be set up to prepare standardized checklists for conducting computer audits in different types of commercial bank branches. Hence a committee was formed under the chairmanship of Shri A. L.Narasimhan, Chief General Manager in - Charge, Department of Banking Supervision, Central Office with participation from RBI, Institute of Chartered Accountants of India, SBI, Citibank and ICICI Bank.

2.7 It was felt that preparing a standardized general checklist for conducting computer audit would have the following benefits:

1. Help the Top Management understand the risks involved in IS area.
2. Be a Reference Document for carrying out IS Audit
3. Demystify the complications involved in the IS Audit process
4. Bring about standardization in IS Audit approaches so as to ensure that required care is taken
5. Help identify different risks involved in the Information Systems

2.8 Standardized checklist would be only in the nature of guidelines and banks would be free to have more elaborate checklists to conduct IS Audit suitable to the IT environment in which they operate and propose to operate. However, the issues elaborated in the checklists would give a fair idea about areas that need to be controlled.

2.9 Different Levels of Computerization

Levels of computerization in the Indian Banking industry vary significantly. On the one hand centrally computerized and fully networked new private banks and foreign banks and on the other with little computerization in old private banks and PSBs are in two ends of the spectrum. However, it would be fair to clarify that there are not many banks with significant assets which would be at the lower end of the spectrum, partly due to the benefits of the technology perceived by the banking industry and the fiat issued by CVC to computerize 70 per cent of business within a target date. Competition in the industry, cutting edge technology based customer services and products, growing customer needs, RBI guidelines, guidelines issued by CVC and VRS offered by Banks are some of the factors that are forcing all the players to computerize the operations quickly and effectively. This sudden spurt naturally brings new risks and thus there is an urgent need to document various risks involved in different levels of computerization, the controls available, the controls needed and the residual risks which the bank after careful consideration of all issues involved is ready to accept. Different levels of computerization could be:

- Centrally Computerized and Fully Networked Banks
- Fully Networked Banks with distributed computing
- Banks offering Internet Banking, POS connectivity etc.
- ATMs including SWADHAN
- Local Area Networked and Wide Area Networked administrative offices
- Fully computerized branches
- Partially computerized branches
- ALPM branches
- PC based branches
- Banks at different stages of SDLC
- Corporate e-mail systems
- Off-shore data processing.

2.10 Computer Audit or IS Audit?

These terms are generally not understood clearly in the industry. Computer Audit would generally mean functional audit in computerized environment and IS Audit would mean the information system audit without the functional focus. It is a common practice in many Public Sector Banks to assign the work of IS Audit to regular Inspectors who do not have commensurate exposure or qualifications to carry out such audit. Growing levels of computerization in the banking industry, complexities of emerging technologies, networking, internet banking etc. necessitate proper IS security and controls in place and regular IS Audits. On the functional aspect also, as most of the operations are computerized, the auditors need to necessarily carry out the audit on computer and computer audit has become day-to-day routine in banking industry.

2.11 Possible areas of audit interest in the IS environment have been broadly classified under different categories and questionnaires have been prepared under each of these categories.

2.12 It was felt by the committee that IS Audit Checklist prepared need to be platform independent and necessary platform dependent control questionnaire can be framed by the Banks themselves. Computer Audit questionnaire also should be Bank independent. On the basis of the practices followed by individual Banks they may frame Bank specific control questionnaire.

2.13 The checklists may be used in conjunction with the IS Audit policy booklet forwarded by DIT, RBI.

1. Business Strategy

1.1 Whether the business strategy is documented and business objectives have been defined and the role of IT has been clearly spelt out in the Business Strategy?

1.2 Whether information technology issues as well as opportunities are adequately assessed and reflected in the organisation's strategy, long term and short term plans.

1.3 Whether assessments are made periodically by the bank to ensure that IT initiatives are supporting the organization mission and goals?

1.4 Whether major developments in technology (hardware, software, communication etc.) are assessed for their impact on the business strategy and necessary corrective steps, wherever needed, are taken?

2. Long Term IT Strategy

2.1 Whether long term IT strategy exists and documented?

2.2 Whether the Long Term plan covers:

- Existing and Proposed Hardware & Networking Architecture for the Bank and its rationale
- Broad strategy for procurement of hardware, software solutions, vendor development and management
- Standards for hardware / software prescribed by the proposed architecture
- Strategy for outsourcing, in-sourcing, procuring off the shelf software, and in-house development
- Information Security architecture
- IT Department's organizational structure
- Desired level of IT Expertise in Banks human resources, plan to bridge the gap, if any
- Strategies converted into clear IT Initiatives with a broad time frame
- IT Costs and cost management
- Plan for transition, if any.

2.3 Whether the Long Term plan is approved by the Board?

2.4 Whether organization structure of IT has been made part of the IT plan?

2.5 Whether IT long-range plan is supporting the achievement of the organisation's overall Mission and Goals?

2.6 Whether a structured approach to the long-range planning process is established?

2.7 Whether the plan is covering what, who, how, when and why of IT?

2.8 Whether prior to developing or changing the long-term information technology plan, management of the information services function have assessed the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses in order to determine the degree to which the existing systems support the organisation's business requirements?

2.9 Whether organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the market, planning horizon, business process re-engineering, staffing, in or out sourcing etc. are taken into account at the time of planning process?

2.10 Whether plan refers to other plans such as the organizational plan and the information risk management plan?

2.11 Whether process exists to timely and accurately modify the long range IT plan taking into account changes to the organisation's plan and in business and information technology conditions?

2.12 Whether a security committee, comprising of senior functionaries from IT Department, Business Group, IT Security Department and Legal Department is formed to provide appropriate direction to formulate, implement, monitor and maintain IT security in the entire organisation?

3. Short Range IT Plans

3.1 Whether long-range IT plans are converted to short-range IT plans regularly for achievability?

3.2 Whether the IT Short-range plan covers the following:

- Plan for initiatives specified in the Long range plan or initiatives that support the long range plans.
- System wise transition strategy.

- Responsibility and plan for achievement.

3.3 Whether adequate resources are allocated for achieving the short-range plans?

3.4 Whether short-range plans are amended and changed periodically as necessary in response to changing business and information technology conditions?

3.5 Whether assessments are made on a continuous basis about the implementation of short range plans?

3.6 Whether clear-cut responsibilities are fixed for achieving the short range IT Plan?

4. IS Security Policy

4.1 Whether a well-documented security policy is available?

4.2 Whether Inventory of IT assets is made part of the policy? Whether inventory of IT assets is kept at branch/ office level?

4.3 Whether policies related to IT activities are listed in the security policy?

4.4 Whether the policy takes into account the business strategy/ plan for the next 3 5 years?

4.5 Whether the policy takes into account the legal requirements?

4.6 Whether the policy takes into account the regulatory requirements?

4.7 Whether the policy is approved and adopted by the Board of Directors/ Top Management?

4.8 Whether the policy is communicated to all concerned and is understood by them?

4.9 Whether the following major security areas are covered in the policy :

- PC and LAN, MAN and WAN security
- Physical Security to IS establishments
- Handling of confidential information
- Handling of security incidents
- Privacy related issues for outside entities
- E-mail security
- Application security
- Interface Security
- Password security
- Operating system security, web site security
- Database security
- Anti virus and piracy policy
- Archived and Backed up data security
- Procedures for handling incidence of security breach
- Disaster Recovery Plan
- Use of cryptology and related security
- Persons responsible for implementing security policy and consequence for wilful violation of the Security Policy.

4.10 Whether a review process is in place for reviewing the policy at periodic intervals and/ or on any other major event?

5. Implementation of Security Policy

5.1 Whether documented security policy is made available to all the levels of users to the extent relevant to them?

5.2 Whether continuous awareness programmes are conducted for security awareness?

5.3 Whether the role of Information Security Officer with responsibilities for implementation of the Security Policy has been assigned?

5.4 Whether detailed procedures for each policy statement are developed?

5.5 Whether suitable methodologies are adopted for implementation?

5.6 Whether suitable security tools are selected for implementation?

5.7 Whether the roles of the implementers are clearly defined?

5.8 Whether the budgetary allocation for implementation of IS security is assessed and documented?

5.9 Whether periodic security audits are carried out?

5.10 Whether on the basis of audit reports or any other vital information suggestions for updating the security policies are conveyed to the right / appropriate management?

5.11 Whether management demonstrates adherence to the Security Policy?

5.12 Whether new entrants are given adequate exposure to the security policy?

5.13 Whether in case breaches of security policy the root cause is analysed and preventive and corrective actions are taken?

5.14 Whether incidence-reporting procedures have been followed?

5.15 Whether the Information Security Officer is made responsible for reporting non-compliance with the approved policy and incidents of security breaches to the Top Management, and to initiate and effect corrective action?

6. IS Audit Guidelines

6.1 Whether a documented and approved IS Audit guidelines are available?

6.2 Whether IS Audit guidelines are consistent with the security policy?

6.3 Whether the IS Audit responsibilities have been assigned to a separate unit, which is independent of IT Department?

6.4 Whether periodic external IS Audit is carried out?

6.5 Whether independent security audit is conducted periodically?

6.6 Whether contingency planning, insurance of assets, data integrity etc. is made part of external audit?

6.7 Whether vulnerability and penetration testing were made part of external audit?

6.8 Whether the major concerns brought out by previous Audit Reports have been highlighted and brought to the notice of the Top Management?

6.9 Whether necessary corrective action has been taken to the satisfaction of the Management?

6.10 Whether adequate training facilities are provided to IS Audit teams so as to enable them to conduct audits effectively?

6.11 Whether IS Audit team is encouraged to keep themselves updated?

6.12 Whether IS Auditors exchange their views and share their experiences internally?

7. Acquisitions and Implementation of Packaged Software

Procurement and implementation of packaged software has various stages in the entire process. The information system auditor (SA) has to familiarize himself with the policies and practices of the bank with regard to software procurement and implementation. The IS Auditor should have prior discussion with the IT Department and should gain the following knowledge before commencing audit work of this area:

- IT Infrastructure and environment in the Bank
- Resources available in the IT Department of the Bank
- Software Products procured and implemented during the period
- Status of the implementations
- Problems if any faced by the users after implementation
- Errors noticed in processing transactions in the procured system
- Any Errors resulting in financial loss, regulatory/ compliance issues, serious customer complaints etc.

Note

This checklist does not address commercial consideration for which regular audit guidelines have to be applied. This checklist is divided into the following Areas:

(a) Requirement Identification & Analysis

(b) Product & Vendor Selection Criteria

(c) Vendor Selection Process

(d) Contracting

(e) Implementation

(f) Post Implementation Issues.

(a) Requirement Identification and Analysis

7.1 Is there an annual plan covering areas requiring computerisation approved by Top Management?

7.2 Is plan in line with the Banks overall IS Strategy?

7.3 Has a functional manager or a committee been identified as responsible sponsors for an area requiring computerisation?

7.4 Have the costs of computerisation been budgeted and included in the overall IT Budget of the Bank?

7.5 Has a detailed plan been made by the IT Department, clearly providing the date of commencement, activities involved, target date of final implementation and estimated costs for each area identified?

7.6 Has this plan been approved by the Sponsor?

7.7 Has a document been prepared clearly detailing the following requirements: Functionality In case of replacement, the problems faced in the existing system and need for replacement Performance Security Operations Risk Mitigation Acceptance Criteria for the System Changes in the operating procedures required to implement the proposed system and persons responsible and plan for effecting the changes Transition/ Migration from existing to proposed plan for a smooth transition Interface requirement with Other Computer Systems.

7.8 Has the requirements been graded as Vital, Essential and Desirable?

7.9 Has the Sponsor approved the requirement document?

(b) Vendor Selection Criteria

7.10 Has the Requirements Document been translated clearly into product acceptance criteria? Has Acceptance Criteria been classified into:

- 'Show Stoppers'
- 'Allowable Customisations'
- 'Desirable positive features'.

7.11 Do the IT Department have a technology standard for product selection?

7.12 Does the Technology standard cover:

- Architecture
- Open Database standards
- Interfaces and API Standards
- Security Standards.

7.13 Are the Product Selection criteria consistent with the IT platform of the Bank? Does the Bank have clearly laid down and approved guideline for selection of product vendors?

7.14 Does the Vendor Selection guideline address the following?

- Market Presence
- Years in operation
- Technology alliances
- Desired size
- Customer base and existing implementation
- Support
- Possibilities of partnership or strategic alliance
- Source code availability
- Local Support in case of foreign vendors.

7.15 Has the selection criteria been decided by the IT Department in consultation with User Departments?

7.16 Has the Sponsor approved the Selection Criteria?

7.17 Does the policy of the bank permit beta-site installations? If yes are criteria for selection distinctly different from regular guideline?

7.18 Does the IT Department use scoring model for evaluating the products and vendor?

7.19 Do the scoring criteria consider the following factors:

- Extent of customisation and work around solutions
- Security Features
- Technology fit
- Performance & Scalability
- No. of installations
- Existing customer reference
- Cost
- Vendor Standing.

(c) Vendor Selection Process

7.20 Does the IT Department have a system to identify potential vendors for an area (such as subscription to magazines; rating reports and reports of specialized agencies such as Gartner, IDC, Data Quest etc.,).

7.21 Are reports of specialized independent rating agencies used for short listing Vendors?

7.22 Does the Bank have a system of floating formal RFP (Request for Proposal) for systems with estimated budget exceeding a certain amount?

7.23 Is there a core team comprising of personnel from IT Department, Functional Departments and Internal Audit

Department in charge of vendor selection and implementation?

7.24 Is the process of selection for each area approved by the Sponsor?

7.25 Are Meetings of the Core Team documented?

7.26 Does Team use prepared check lists for

(a) Product Evaluation

(b) Site Visits

(c) Customer Reference

7.27 Is final evaluation and selection fully documented and approved by the Sponsor?

7.28 Does the document clearly reflect the rationale used for the selection?

(d) Contracting

7.29 Does the bank have approved terms and conditions for Product Licensing Agreements?

7.30 Do the Licensing terms contain:

a) Escrow mechanism for Source codes

b) Facilities for minor customisation

c) Maintenance and Upgrades.

7.31 Does the Bank have a Service Level Agreement with Product Vendors for Support and Maintenance?

7.32 Where the contract is entered with a Distributor or Reseller is there a commitment to ensure that the actual owner would support the Bank in case of relationship between the owner and the reseller breaks?

7.33 Does the contract clearly segregate duties and responsibilities of the Bank and the Vendor?

7.34 Does the contract include a clause to protect the Bank from the Vendor using the bank data?

7.35 Does the contract clearly specify the product base lines?

(e) Implementation

7.36 Is gap analysis between the requirement and the selected product carried out and documented?

7.37 Does this document act as the basis for further implementation plans?

7.38 Does the Bank's policy provide for parallel run of previous system during the implementation period?

7.39 Is there an agreed plan for implementation? Has the plan been approved by the Sponsor, Vendor and IT Department?

7.40 Does the implementation plan clearly identify product customisation requirements, user acceptance criteria and test for such customisation?

7.41 Does the implementation plan address data migration from previous systems?

7.42 Does the implementation cover the following?

a) User Departments' involvement and their role

b) User Training

c) System Administration Training

d) Acceptance Testing

e) Role of Vendor and period of Support

f) Required IT Infrastructure plan

g) Risk Involved and actions required to mitigate risks.

7.43 Does the responsibility for accuracy of key parameters / Static Data rest with the functional department?

7.44 Is there a list of areas, which will be controlled by the Vendor during the implementation phase?

7.45 Does Bank have a test environment to simultaneously allow familiarisation during the implementation process? Have errors identified during the implementation phase been documented and the root cause of the errors analysed and confirmed by the Software Vendor?

7.46 If there are bugs and errors due to design flaws, are they escalated to higher levels in Software Vendors' organisation and the bank?

7.47 Is Test packs developed by user groups for testing customisation delivered by the vendor?

7.48 Is there a clearly identified data integration strategy during customisation period? (If customisation involves additional elements of data to be captured)

7.49 Is the result of testing properly documented?

7.50 Are necessary changes to System documents carried out on customisation?

7.51 A re all following documents handed over by the Vendor?

- System Documentation covering Design and Program Documentation
- Data Dictionary
- Installation Manual

- User Manual
- Trouble Shooting.

7.52 Does the IT Department have a proper archival system for these documents?

7.53 In cases where source code is given by the Vendor, has the IT department done a Technical conversion and issued a confirmation of satisfactory compilation/performance?

7.54 Is there a system to issue formal Acceptance Certificate signed off by User Department, IT Department and the Sponsor?

(f) Post Implementation Issues

7.55 Has the IT Department taken the required consequential action for Back ups, Disaster Recovery and Performance Tuning?

7.56 If Source codes are delivered, are the source codes base lined as per IT Department Procedures?

7.57 Has the IT Department in consultation with User Department worked out Database Controls?

7.58 Has IT Department introduced a system to track problems reported by users, escalation to vendor and their resolution?

7.59 Is there a system of measuring vendors' support with the agreed service levels?

7.60 Is there an identified System Administrator who is responsible for managing access to the system, back up and ensuring data base controls?

8. Development of Software In-house and Out-sourced Audit framework for Software developed in-house Software Audit Administration

8.1 Is the software audit (SA) conducted using pre-designed formats at three levels viz.

a) Program Level

b) Application Level and

c) Organization Level.

8.2 Has IT department adopted any Standardised quality processes such as ISO, SEI CMM etc., for Software development?

8.3 Has Non compliance reported in such quality audit are properly attended to and rectified?

8.4 Is there a system in place to reveal the outcome of the audit to the staff of the Bank at respective levels?

8.5 Whether a structure is in place for effective Software Audit so that reliable results can be obtained?

Software Audit Process

Audit at Program Level

8.6 Are the programs developed by drafting the formal specifications, defining scope, application, input data elements, output requirements, process workflow etc.?

8.7 Is software tested for quality assurance?

8.8 Is quality assurance team different from development team?

8.9 Are data / test results preserved for future reference?

8.10 Are there temporary patches developed by just copying a few set of legacy programs? If so, are they tested properly before deployment and limitations and conditions, which such programs cannot handle, is communicated to users and appropriate control procedures are put in place?

8.11 Do all the program source codes contain a Title area, specifying the author, date of creation, last date of modification and other relevant information?

8.12 Are there adequate input validation checks built into data entry programs?

8.13 Whether the following manuals are prepared? Systems operations / Installation Manual User Manual

8.14 Are there well-established testing procedures? Does the testing procedures cover:

- What, When and How to Test?
- Positive (Test done by processing valid data and checking if the results are accurate) and Negative Testing? (Test done by processing invalid data and checking if the program generates necessary error messages)
- Performance and scalability?
- Recording and maintaining test results?

8.15 Whether parallel testing at a few pilot installations done after completing pre implementation testing?

8.16 Whether programs successfully implemented have passed the test for accuracy of outputs generated?

8.17 Whether the source code location with ownership for future up-gradation is well established?

8.18 Whether every patch/ update is authorized by a competent authority?

8.19 Whether the development consider security requirement as per approved security policy?

Audit at Application Level

8.20 Are operational controls such as distinct user passwords are in place and are enforced?

8.21 Whether necessary 'Regulatory Compliance' requirements have been taken into account by the user?

8.22 Whether SRS has taken into account the Error/ Fraud / Disclosure / Interruption / Organisational Risks etc.?

8.23 Whether input / output controls are in place?

8.24 Are validation controls are in place, viz. Field/ Transactions/ File with appropriate error reporting?

8.25 Are appropriate data classifications with security in place, viz. Read only for users, Read/ Write for authorized persons?

8.26 Is audit trail built into the systems?

8.27 Does the system provide for 'exception reporting'?

8.28 Whether adequate firewalls set up to ensure that any outside access being provided is limited in scope ad does not intrude on sensitive data areas?

8.29 Whether user acceptance is recorded along with test plan data / test data / test results for future reference?

8.30 Whether the user sign off has been obtained?

Audit at Organisational Level

8.31 Is updated organizational chart being kept?

8.32 Are the duties of developers and operators of the system distinctly segregated?

8.33 Is job rotation in place?

8.34 Whether software implementation plan has been approved by the controlling authority?

8.35 Whether provision has been made for maintenance of software library?

8.36 Is there a system in place for software distribution?

8.37 Are error reporting and control mechanisms in place?

8.38 Is there a system for post completion 'Review Audit'?

8.39 Is there a standard and secure procedure for up-keep of source / object code?

8.40 Are security controls including Disaster Recovery in place?

8.41 Is the data conversion audited?

8.42 Are all changeovers from one system to another system authorized by a competent Authority?

8.43 Are the training requirements for users properly identified?

8.44 Is the DRP in place at all operating offices?

8.45 Are documentations available at operational stage to facilitate formal changeover of jobs?

Audit Framework for Software Outsourcing

8.46 For software development outsourcing, are there laid down criteria for selection of Vendors?

8.47 Whether formal outsourcing strategy for necessary interface with the vendor is in place?

8.48 Is the outsourcing activities evaluated based on the following practices:

- What is the objective behind Outsourcing?
- What are the in-house capabilities in performing job?
- What is the economic viability?
- What are the in-house infrastructure deficiencies and the time factor involved?
- What are the Risks and security concerns?
- What are the outsourcing arrangement and fall back method?
- What are arrangements for obtaining the source code for the software?

8.49 Is there formal approval system in place from the Head of the user department?

8.50 Does the user department representative 'Expert Officer' visit the vendor's premises for reviewing the capability and quality of software development activities?

8.51 Does the vendor present the progress of software development at periodic intervals?

8.52 Is there a formal product hand over and project completion system in place?

8.53 Is there an Agreement entered by the Bank with the Vendor for completion of the software development in time. Whether any penalty clause exists for delayed completion of work?

9. Physical Access Controls

9.1 Whether there is a policy regarding physical access control and is a part of the security policy of the organisation?

9.2 Whether there is a mechanism to review the policy regularly?

9.3 Whether the policy on the following are appropriate:

- Lay out of facilities
- Physical and Logical Security
- Safety
- Access
- Maintenance
- Signage
- Visitors
- Health
- Safety and environmental requirements
- Entrance and exit procedures
- Regulatory requirements
- Legal requirements.

9.4 Whether the Information System facility located in a place, which is not obvious externally?

9.5 Whether the facility is located in least accessible area or / and access is limited to approved personnel only?

9.6 Whether the physical access control procedures are adequate for employees, vendors, equipment and facility maintenance staff?

9.7 Whether 'Key' management procedures and practices are adequate? Whether review and updates are carried out on a least access needed basis ?

9.8 Whether the access and authorization policies on the following adequate? Entering/ Leaving Escort Registration Visitor passes Surveillance cameras

9.9 Whether the policies laid down are implemented?

9.10 Whether periodic review of access profiles is carried out?

9.11 Whether revocation, response and escalation process in the event of security breach appropriate?

9.12 Whether security for portable and off-site devices adequate?

9.13 Whether control of visitors adequately addressed? Whether issues like registration, pass, escort, logbook for check in and check out are handled properly?

9.14 Whether fire prevention and control measures implemented are adequate and tested periodically?

9.15 Whether computing facilities are situated in a building that is fire resistant and wall, floor and false ceiling are non-combustible?

9.16 Whether smoking restriction in computing facilities are in place?

9.17 Whether smoke/ heat-rise detectors installed and connected to the fire alarm system?

9.18 Whether fire instructions are clearly posted and fire alarm buttons clearly visible? Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?

9.19 Whether fire drill and training are conducted periodically?

9.20 Whether computing facilities are located above ground level? Whether water leakage, seepage etc. are prevented?

9.21 Whether air-conditioning, ventilation and humidity control procedures in place, tested periodically and given adequate attention

9.22 Whether security awareness is created not only in IS function but also across the organisation?

9.23 Whether physical security is continually addressed and whether physical security is ensured at suppliers facilities also in cases where organisation's' assets either physical or data are processed at supplier's facilities?

9.24 Whether UPS is available? If so, is it covered under maintenance?

9.25 Whether alternate or re-routing telecommunication lines are available?

9.26 Whether alternative water, gas, air-conditioning and humidity resources are available?

9.27 Whether all access routes are identified and controls are in place?

9.28 Whether the computer room is locked and access is restricted?

9.29 Whether appropriate holidays and vacation are availed by the IT staff?

9.30 Whether hazardous commodities are not stored in the IS area?

9.31 Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data/ information on them?

9.32 Wherever access to the IS facility is enabled through ID cards/ badges, etc., are there controls to ensure that the issue and re-collection of such access devices are authorised and recorded.

9.33 In case of outsourced software, whether all maintenance work is carried out only in the presence of/ with the knowledge of appropriate bank staff?

9.34 Based on criticality of the IS facility, are there video surveillance equipments to monitor the movements of the personnel inside the facility? If so, check whether continuity of video recording is ensured.

9.35 Whether access violations are recorded, escalated to higher authorities and appropriate action taken.

10. Operating System Controls

Adherence to Licensing Requirements

10.1 Whether the Branch/ Office holds the original license from the Head Office/ Vendor for using the operating system software?

10.2 Whether the original Operating System Media supplied by the vendor is available in the Branch/ Office?

10.3 Verify all the manuals and user guides provided by the vendor at the time of supply of the system and ensure whether all are physically available. Ensure that proper library records are maintained by the Branch/ Office for all the manuals/ books received along with the package.

10.4 Ensure whether the number of licenses used in the Branch/ Office is less than or equal to the number of user licenses mentioned by CPPD/ Vendor in the license

Version Maintenance and application of patches

10.5 Verify the system configuration such as Memory, Clock speed, Hard Disk size, OS version, etc. and ensure that they are as per order or terms stipulated by CPPD/ IT Department at the time of procurement.

10.6 Ensure that the latest OS version is running at the site. Check whether latest updates/ patches released by the OS vendor have been applied.

Network Security

10.7 Check if the system being audited trusts other hosts for providing logon access to similar user accounts (same user account in the system being audited and the host system) in both the systems without supply of password. If so, ensure that it has been implemented in accordance with IT/ CPPD guidelines only.

10.8 Check if remote logon is enabled and if so, whether it is as per the guidelines of CPPD/ IT Department. Ensure that the users logging on from remote locations are identifiable by terminal IDs/ IP addresses.

10.9 Check if remote logon through services such as ftp, telnet, etc. is disabled. If not, ensure that the same has been implemented as per IT security policy of the Bank.

User Account Maintenance

10.10 Each and every user ID in the operating system level should have been created only after specific approval of the Branch Manager/ Department head in writing on a request form signed by the respective user. Verify whether such approval is in place for all the active user IDs.

10.11 Apart from the approved request forms, the Branch/ Office should be maintaining a user profile register with details such as:

- Employee Name
- Designation
- Employee Number
- Date of joining the Branch/ Office
- User ID allotted
- Date of creation of user ID
- Date of deletion of user ID
- Signature of the user
- Initials of the DBA.
- Initials of the BM.

Verify whether the above-mentioned register is maintained. All the entries in the register should be accounted for in the list of active user IDs obtained from the operating system.

10.12 Check that with the exception of reserved user accounts created for the internal use of the operating system, RDBMS, Application system, etc., all other user accounts are uniquely identifiable by the respective user's personal name. In other words, generic user accounts, which cannot be attributed to any individual, should not be allowed. Verify this and comment.

10.13 Check the operating system user IDs which have security equivalence to Super User and ensure whether they are permissible as per CPPD/ IT Department guidelines.

10.14 Check whether all the user IDs is protected with passwords.

10.15 With the exception of Super User account, check whether all default system login accounts are disabled. In other words, ensure whether all default vendor accounts shipped with the Operating System have been disabled. This should be checked after each upgrade or installation.

10.16 Check the list of active user groups and ensure that general users are not members of sensitive/ privileged user groups which have higher privileges.

Logical Access Controls

10.17 Ensure that access to operating system command prompt is disabled for general users in the Branch/ Office.

10.18 If some or more of the system administration related activities are driven through a menu-based utility assigned to any user ID, which is privileged, ensure that such ID(s) cannot be used to bypass login security and access the command prompt.

10.19 Ensure that the file pertaining to each user containing login parameters cannot be modified by the respective user.

10.20 Ensure that any user other than the Super User cannot modify the system activity log file.

10.21 Check whether access rights to system files, application executable program files, application data files, utilities, application parameter files, system/database configuration/ initialisation files, etc. have been adequately controlled to allow read/ write/ execute/ modify, etc. as the case may be to appropriately authorised users on need to know, need to do basis.

10.22 Obtain a list of world write able (directories/ folders with access to every user) directories/ folders in the system and ensure that they have been set only in accordance with IT/ CPPD guidelines.

10.23 Verify the access rights settings for the users' home directories and ensure that they are not owned by any ID other than the actual user. Also, ensure that user's home directory cannot be accessed by any other user.

System Administration

10.24 Ensure that the facility to logon as Super User is restricted to system console for security reasons.

10.25 Check the password definition parameters included in system and ensure that minimum password length is specified according to the IT security policy of the Bank (ideally, at least six characters).

10.26 Ensure that the maximum validity period of password is not beyond the number of days permitted in the IT Security policy.

10.27 Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.

10.28 Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.

10.29 Verify if the parameters to control the password format has been properly set according to security policy of the Bank.

10.30 Verify the parameters in the system to control automatic log-on from a remote system and ensure whether they have been properly set according to security policy.

10.31 Verify the parameters in the system to control the number of concurrent connections a user can have simultaneously from different terminals and ensure that it is restricted as per CPPD/ IT Department guidelines.

10.32 Examine the terminal inactive time allowable for users and verify if the time set is in accordance with the guidelines.

10.33 If minimum password validity period is not set properly, verify the latest date of change of privileged passwords including Super User and ensure that the password is not too old, in any case not older than a month.

10.34 Check whether automatic logging of user activities is enabled.

10.35 Check for unexpected users logged on to the system at odd times.

Maintenance of Sensitive User Accounts

10.36 Ascertain as to who is the custodian of sensitive passwords such as Super User and verify if he/ she is maintaining secrecy of the password, whether he/ she has preserved the password in a sealed envelope with movement records for usage in case of emergency.

10.37 From the log file, identify the instances of use of sensitive passwords such as Super User and verify if records have been maintained by the Branch/ Office with reason for the same. Ensure that such instances have been approved by CPPD/ TBC Group/ IT Department and whether Branch Manager, Password Custodian and DBA have signed the record.

10.38 From the log file, identify the instances of unsuccessful logon attempts to Super User account and check the terminal ID/ IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations.

11. Application Systems Controls

The application system before being implemented has to be reviewed by the auditor if various controls suggested by Users are incorporated in the application system. The various controls, which have to be included in the system are as follows:

- Logical Security
- Input Controls
- Processing Controls
- Output Controls
- Authorisation Controls
- Interface Controls
- Data integrity/ File continuity Controls.

Logical Access Controls

11.1 Does the software allow creation of user-IDs in the same name more than once?

11.2 Does the software encrypt the passwords one way and store the same in encrypted form?

11.3 Does the software display the password as it is keyed in?

11.4 Does the software lock the user-ID if it is used for 3 unsuccessful times to logon to the system?

11.5 Does the software force the User to change the password at set periodical intervals?

11.6 Does the software maintain password history i.e., does not allow the same password to be used again on rotation basis?

11.7 Is there any audit trail for the maintenance of User profiles?

11.8 Does the software have provision to create and maintain user-IDs based on users' designations and positions held?

11.9 Can DBA change other's password? If so is it reflected in the audit trail?

11.10 If a user-id record is deleted, does the software delete it physically or logically? Does the software capable of producing a report of logically deleted User-IDs?

11.11 Does the software have provision to restrict different menu options to different user-Ids based on user level (based on designation/ powers, etc.)?

11.12 Does the software have provision for defining access rights to users such as, Read Only, Read and Write, Modify, Delete, etc.?

11.13 Verify who can do the User Profile Maintenance? Does the system give facility to general users also to do user profile maintenance?

11.14 Does the software tag each and every transaction with the user-IDs of maker and checker?

11.15 Does the software allow the same user to be both maker and checker of the same transaction? If so, does the software produce an exception report of transactions with same maker and checker IDs?

11.16 Are the User-IDs reflected in the contents of the report printed?

11.17 Does the software allow automatic logical deletion of inactive users after certain period of time?

11.18 Does the system maintain password length to be of minimum 6 or 8 characters or as indicated in the password policy?

11.19 Can the user-IDs be created without passwords?

11.20 Does the system limit the maintenance of system control parameters to privileged user level having sufficient authority only?

Input Controls

11.21 Whether each transaction is recorded in such a way that it can be subsequently established that it has been input (e.g., Tran ID etc)?

11.22 Does the software have controls to ensure that all recorded transactions are:

11.22.1 Input to the system and accepted once and only once.

11.22.2 If transactions are rejected, they are reported.

11.23 Are there adequate procedures to investigate and correct differences or exceptions identified? Are there adequate procedures to investigate and if necessary, correct the following:

- Missing and possible duplicate transactions disclosed by the input control.
- Rejected items.

11.24 If corrections are made to rectify differences, exceptions, duplicate transactions, missing transactions and rejected items, are they approved (e.g., maker/ checker, exception report, etc.)?

11.25 If the input of data is through batch upload, does the software have controls to ensure that all the entries in the batch have been uploaded without any omission/ commission (e.g., reconciliation of control totals, etc.)?

11.26 Does the software have adequate controls to ensure that, data have been accurately input (e.g. range checks, validity checks, control totals, etc.)

11.27 Verify the controls to ensure compatibility of data when they are input at two or more modules and are correlated. (e.g. if the customer category in customer master is stated as “Staff”, the rate of interest in the account master for the same customer should have appropriate code applicable to staff and system should not allow other codes).

11.28 Verify the consistency/ concurrency of user inputs, if two users are accessing the same record at the same time.

11.29 Verify if the inputs can be captured for various conditions. (e.g. if signatures can be captured for single A/c, Joint A/c etc).

11.30 Verify the controls over system-generated transactions through user processes (e.g. verification of outputs containing system generated transactions and authentication by branch officials).

11.31 If user controls are relied upon to ensure the controls over complete and accurate input of data, are these controls adequate and operative continuously?

Processing Controls

11.32 Does software have adequate controls to ensure that all transactions input have updated the files?

11.33 If user controls are relied upon to ensure the controls over complete and accurate update of files with data, are these controls adequate and operative continuously?

11.34 Are there adequate procedures for investigation and correction of differences or exceptions identified by the controls over update for completeness and accuracy?

11.35 Are such corrections approved?

11.36 List out the events that cause the transaction to be generated (e.g. input of a parameter such as a date, attainment of a condition, etc.), the key data used as a basis for the generation, and the programmed procedures that perform the generation. (e.g., in the interest calculation process, generally, the user will run the interest run job and the system will take the customer balances (key data) and apply interest rates (key data) and debit/credit the interest. The program, which performs these activities, should be logically sound so that no processing errors are introduced).

11.37 For the key data outlined above, are there adequate controls to ensure that the key data used as a basis for the generation of data are complete and accurate?

11.38 Where applicable, whether the key data is authorised by appropriate level of users and kept secure?

11.39 For the programmed pr5ocedure that generates the data, if user controls are relied on to check the accuracy of the generation process, are these controls adequate?

11.40 Are there adequate procedures to investigate and correct any differences or exceptions identified by the controls over the completeness and accuracy of generation? Are the corrections approved?

11.41 Is there any restart facility for batch jobs if they terminate abruptly? Are there controls to ensure that no errors are introduced during restart?

11.42 Is the User-ID of the person who executes the batch job embedded in the transactions?

11.43 If the process has to be done only once, does the software ensure that the process is not executed more than once?

11.44 Is there any day begin, day end process? If so, are these processes logically sound to carry out the designed objectives completely and accurately?

11.45 Are the transactions for the day identifiable?

11.46 Does the software ensure sequencing of processes? i.e., does the software ensure that processes are not initiated out of sequence.

11.47 If certain processes are compulsory, does the software ensure that all such processes are completed before triggering the day end process?

11.48 Verify if there is an event log for the batch processes.

11.49 Verify if the application is able to handle processing at peak times (e.g. is the application capable of handling progressively increasing volumes).

11.50 Verify if software maintains audit-trail to uniquely trace any modification/ deletion/ addition with user-ID.

11.51 If updates occur in more than one file or table, if the process interrupts, verify if there is a roll back.

11.52 Verify if the application maintains adequate control over security items such as DDs/ Pay Orders/ Branch advices, etc.? Are they reconciled and exceptions identified and reported?

Output Controls

11.53 Verify the format, contents, accuracy and utility of the reports generated by the system.

11.54 Verify if there is any provision for generating exception transactions statement from the system.

11.55 If the output has more number of pages and if printing is interrupted, is there any provision to restart the printing from that page.

11.56 Verify if outputs can be viewed/ generated by users only on need to know basis. In other words, check whether outputs cannot be generated by all and sundry users in the system.

11.57 Check the controls exercised by the user (Branch/ Office) on the generation, distribution, authentication and preservation of computer outputs and comment on the adequacy of the same.

11.58 Check whether the application is keeping adequate controls over computer generated outputs lying in print queue/ spool.

11.59 Does the output contain key control information necessary to validate the accuracy and completeness of the information contained in the report such as last document reference, period, etc.?

Interface Controls

11.60 If the data has to be transferred from one process to another process, verify if no manual intervention is possible and no unauthorised modification to data can be made.

11.61 Verify the mode of transfer of data from one process to another i.e. through floppy or through mail.

11.62 Verify the effect when one process is down and the interface is working

11.63 Is there a periodic system of ensuring consistency of data from process from which it is transferred to the process to which it is transferred?

Authorisation Controls

11.64 If the transaction is authorised by software itself under specific conditions, are the programmed procedures logically sound to ensure that all authorisations take place as expected only.

11.65 Does the software prevent the same user from performing both the functions of entering a transaction and verifying the same?

11.66 If transactions are authorised manually, are there controls to ensure that a) they are properly authorised by an independent and responsible official and b) no unauthorised alterations are made to authorised transactions?

11.67 If manually approved transactions are authenticated by the input of a password, are passwords adequately controlled?

11.68 Do access rights reflect the appropriate authority limits?

11.69 If the transaction is identified by the system as requiring supervisory approval and is, therefore, routed to a queue file pending review and release by a responsible official, are the procedures for identifying 'items needing approval' adequate to identify all such transactions?

Data Integrity/ File Continuity Controls

11.70 Whether hash total is used to verify the continued integrity of data? Is the total of the items on data file regularly reconciled to an independently established total (e.g. agreement to a manual control account or computer agreement to a control record) on a suitable timely basis to ensure that there is no tampering of data.

11.71 Are there adequate procedures to investigate and correct differences disclosed by the above-mentioned reconciliation.

11.72 Verify if the entire record after commit can be physically deleted (it should not be allowed).

11.73 If the software keeps record of security items, are there adequate controls to ensure the complete and accurate recording of security items in the system?

11.74 Are the programmed procedures, which utilise the security items in the system, logically sound so that there are no errors?

11.75 Are all asset movements supported by suitable written authorisations?

12. Database Controls

It is important to ensure the following with reference to databases:

- Database is physically secure and free of any corruption.
- Access to the database is restricted and permitted only to authorized personnel.
- Referential Integrity of the data is ensured at all times.
- Accuracy of the contents of the database is verified periodically.
- Database is also technically verified periodically, in terms of storage space, performance tuning and backup.
- Backups of the database are periodically retrieved and ensured that they are in order.

This checklist is divided into following areas:

- Physical access and protection.
- Referential Integrity and accuracy.
- Administration and House Keeping.

Physical Access and Protection

12.1 Is there a list of databases with the names of administrators, which the bank recognizes:

(a) Mission Critical Systems such as Internet Banking, Core Banking etc., ATM Base 24 Database

(b) Essential Systems such as Credit Card Processing Systems (Which operate on the near online mode)

(c) Reporting Systems such as Data Warehouse, EIS Reporting

12.2 Is there joint responsibility of the user department and the

IT Department for administration of mission critical databases?

12.3 Does IT Department identify and segregate hardware hosting these databases and whether these hardware resources have been year marked?

12.4 In case if the same hardware is used at branches or other locations whether there are clear partition between application area and data area?

12.5 Does the IT Department have a laid down standards/ conventions for database creation, storage, naming and archival?

12.6 Are Database administrators at responsible levels in the bank?

12.7 For database access, is the OS level file and directory permissions restricted as required for the application?

12.8 Are users denied access to the database other than through the application?

12.9 Whether use of triggers and large queries monitored to prevent overloading of database and consequent system failure?

12.10 Are direct query/ access to database restricted to the concerned database administrators?

12.11 Are all vendor-supplied passwords to the default users changed? Have all demo user and demo databases removed?

12.12 Are there controls on sessions per user, number of concurrent users etc?

12.13 Is creation of users is restricted and need based? Are the rights granted to various users reasonable and based on requirement?

12.14 Is the database configured to ensure audit trails, logging of user sessions and session auditing?

12.15 Does the administrator maintain a list of batch jobs executed on each database, severity of access of each batch job and timing of execution?

12.16 Are Batch Error Logs reviewed and corrective action taken by the Administrator periodically?

12.17 Is there a separate area earmarked for temporary queries created by power users or database administrator based on specific user request?

12.18 Are temporary sub databases created removed periodically or after the desired purpose is achieved?

12.19 Does the design or schema of all tables/ files in database contain fields for recording makers, checkers and time stamp?

12.20 Are database administrators rotated periodically?

12.21 In cases where customer data is provided to external service providers does the bank have confidentiality undertakings from these service providers?

Referential Integrity and Accuracy

12.22 Are there standard set of database control reports designed in consultation with the user department for ensuring accuracy and integrity of the databases? E.g.:

a) Total of transactions and balances;
b) Record Counts
c) Hash Totals.

12.23 Are these reports run directly from the back end database periodically and the results both positive and negative are communicated by the Administrators to Senior Management Personnel?

12.24 Are these reports run periodically and taken directly by the User Department themselves to ensure accuracy?

12.25 In case of automated interface between systems is there a system of reconciliation between the source and receiving system for critical information?

12.26 Is there a system of periodic reconciliation between Sub databases and the GL Database of the bank?

12.27 In cases where data is migrated from one system to another has the user department verified and satisfied about the accuracy of the information migrated?

12.28 Is there a formal data migration report?

12.29 Are there entries directly made to the back end databases? If they are made under exceptional circumstances, is there a system of written authorization?

12.30 If entries in the database are updated/ deleted due to any exceptional circumstances (e.g. during trouble shooting, etc.), are they approved in writing and recorded?

Administration and House Keeping

12.31 Does the System Administrator periodically review the list of users to the database? Is the review documented?

12.32 Are inactive users deactivated?

12.33 Is there back up schedule?

12.34 Are databases periodically retrieved from the back up in test environment and accuracy ensured with the physical environment?

12.35 Are senior personnel from the user department involved in testing backup retrieval?

12.36 Is there periodic purging / archival of databases?

13. NETWORK MANAGEMENT PROCESS

13.1 Is there an Information Security guidelines document, which defines the minimum configuration for any device/ link on the bank's network, including levels of encryption?

13.2 Are all platforms/ links/ devices in compliance with the guidelines? If not, has an appropriate level of management reviewed the non -compliant parts of the network to ensure that the risk levels are acceptable?

13.3 For all items supported by external vendors, does the vendor or the manufacturer verify that all cryptographic functions in use by the product/ service, such as encryption, message authentication or digital signatures, use Corporate IT Department approved cryptographic algorithms and key lengths.

13.4 Wherever applicable, whether background and reference checks for both internal and outsourced vendor staff that perform security-related functions for the product/ service under review are carried out. This includes job applicants who have accepted a job offer, temporaries, consultants, full time staff as well as the outsourced vendor who is involved in product/ service management and operations.

RISK ACCEPTANCE (Deviation)

13.5 Does the Bank have a Risk Acceptance process wherein all the identified risks are documented and approved for any non-compliant issue that cannot be remedied and where effective compensatory controls exist?

AUTHENTICATION

13.6 Does the product/ service authenticate (verifies) the identity of users (or remote systems) prior to initiating a session or transaction? Have these Authentication mechanisms been approved by then Bank's IT Department? (These include Personal Identification Numbers (PINs), passwords (static and dynamic), public keys and biometrics.)

13.7 Does the Bank verify that the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT Department and required compensating controls have been implemented?

Passwords

13.8 Does the Bank have a comprehensive password construction, implementation and management policy?

Personal Identification Numbers (PINS)

13.9 Does the Bank have a policy for the Personal Identification Numbers, used by various set of customers who access the Banks systems directly using channels like ATM, Phone banking, Internet banking, Mobile banking etc?

Dynamic Passwords

13.10 Do the products/services using dynamic passwords for authentication, use an IT Department approved authentication server to validate the password?

Public Key Infrastructure (PKI)

13.11 Do the products/ services using Public key (or asymmetric) cryptography for authentication either on a session basis (peer authentication) or on a per message/ transaction basis (digital signatures) use approved security protocols to comply with the Public key technology standard?

13.12 For products/ services that use PKI, private keys, which are stored in hardware or software, must be protected via an approved mechanism. The protection mechanism includes user authentication to enable access to the private key.

13.13 For products/ services that use PKI, an approved process for verifying the binding of a user identity to the public key (e.g., digital certificate) is required for any server relying on public key authentication.

Biometrics Authentication

13.14 Do the products/ services utilizing biometrics authentication only use biometrics for local authentication?

ACCESS CONTROL

13.15 Is the access to highly privileged IDs (e.g., system administration access) strictly controlled, audited and limited in its use?

13.16 Does the product/ service support the need to perform a periodic entitlement review? A periodic entitlement review process should validate access privileges.

13.17 Does the product/ service support the requirement to limit individual user sessions to a maximum of X minutes of inactivity using either session time out or a password protected screen saver.

13.18 Is there a process in place to ensure that access rights reflect changes in employee or job status within X hours of the change? This includes physical access tokens and dial-in capabilities as well as any systems or applications.

13.19 Does the product/ service supports the ability to disable external customer user IDs after X months of inactivity and deleted after Y months of inactivity unless they are extended through the explicit written approval of the business.

13.20 For any products/ services, which has been outsourced, Is there a process in place to ensure that all platforms, services and applications are configured to meet Bank's Information Security Standards?

13.21 Does the product/ service display the (A) date and time of last successful login and (B) the number of unsuccessful login attempts since the last successful login.

13.22 Does the product/ service support a periodic process to ensure that all user IDs for employees, consultants, agents, or vendors are disabled after X days and deleted after Y days from the day they were not used unless explicitly approved by the business.

CRYPTOGRAPHY

13.23 Is there a cryptography/ encryption policy for various types of classified information that travels/ gets stored within and outside the Bank's network(s)?

NETWORK INFORMATION SECURITY

13.24 Have the Network data monitoring tools (e.g., sniffers, data scopes, and probes) utilized by the product/ service been approved by the Bank's IT Department?

13.25 Is the approved Legal Affairs banner being displayed at all entry point where an internal user logs into the product/ service? An automated pause or slow roll rate is in place to ensure that the banner is read. The Legal Affairs Banner usually carries the following kind of text:

"You are authorized to use this system for approved business purposes only. Use for any other purposes is prohibited. All transactional records, reports, e-mail, software and other data generated or residing upon this system are the property of the Company and may be used by the Company for any purpose. Authorized and unauthorized activities may be monitored."

NOTE:

This is required for all mainframe, mid-range, workstation, personal computer, and network systems.

13.26 Has dial-in connectivity been prohibited on network-connected machine (server and workstation) except where documented and explicitly approved in writing by Business Management and the IT Department. When explicitly approved, the modem must, as a minimum control, prohibit answer or pickup until after the 5th ring.

13.27 Have the remote control products used in a dial in environment been approved by the IT Department explicitly?

13.28 Is it ensured that only software (applications/ operating systems etc.) supported by the vendors only is used? (Unsupported software could be vulnerable to attacks since the vendors would not come up with the relevant patches)

13.29 Is the Anti-Virus software configured to check viruses even from the floppy drive/ CD ROM drive?

E-MAIL AND VOICE MAIL RULES AND REQUIREMENTS

13.30 Is there a policy that covers e-mail & voice mail transmission of data?

13.31 Whether there are procedures, which require that all the incoming e-mail messages be scanned for virus to prevent virus infection to the Bank's network?

13.32 Whether all e-mails are identified with a user's name or e-mail ID to facilitate tracking? Whether e-mail ID allotted to a user is prevented from being used by another user?

13.33 Ensure that users do not forward the e-mail messages automatically without prior approval.

13.34 Whether there are procedures to ensure that users do not send confidential or sensitive information via e-mail? Whether the information transmitted through e-mail is encrypted?

13.35 Whether all e-mails sent and received by employees via Bank's network are treated as Bank's records? Is there procedure to monitor them?

INFORMATION SECURITY ADMINISTRATION

13.36 Is there an approved document clearly outlining the Information Security Administrator's (ISA) responsibility?

13.37 Are all the administrative actions (e.g., adding/deleting users, changes to entitlements/passwords) backed up by an independent review?

13.38 Does the ISA function review all security audit logs, incident reports, and on-line reports at least once per business day?

13.39 In case of Wide Area Networks (WAN), are the router tables maintained securely in Routers?

13.40 Are router login IDs and passwords treated as sensitive information and managed by authorised administrators?

13.41 Are all changes to router table entries logged and reviewed independently? Are access violations taken note of, escalated to higher authority and acted upon in a timely manner?

13.42 Is there a process to report all unusual or suspicious activity? (Reporting to IT Department, investigating immediately, and bringing the case to closure without delay)?

13.43 Does the ISA function assesses compliance with their security procedures quarterly and reports their results to the IT Department?

13.44 Have all the all security related administrative procedures under the control of the ISA been documented and approved by management (annual exercise)? At minimum procedures should include:

- Information Ownership
- Data Classification
- User registration/ Maintenance

- Audit Trail review
- Violation logging and reporting
- Sensitive activity reporting
- Semi-annual Entitlement Reviews
- Password resets
- Escalation reporting.

MICROCOMPUTER/ PC SECURITY

13.45 Does the LAN servers, mail servers, and microcomputers have IT Department approved anti-virus products installed?

13.46 Are all product/ service specific microcomputers/PCs secured against removal and theft commensurate with the value of the computer and information it holds along with a process to report any thefts to the IT Department?

13.47 Are microcomputers/ PCs having sensitive information protected with power on password to prevent unauthorised access?

13.48 Are sensitive data in such microcomputers/ PCs backed up and preserved properly with records to ensure recovery in case of failure?

AUDIT TRAILS

13.49 Does the audit trail associate with the product/ service support the ability to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, highly privileged accounts and emergency IDs?

13.50 Does the financial transactions as well as additions, changes and deletions to customer's demographic data/ important statistics, get recorded in the product/ service audit trail?

13.51 Does the audit trail for product/ service record all identification and authentication processes? Also Is there a retention period for the Audit trails

13.52 Does the audit trail associate with the product/ service log all actions by the ISA?

13.53 Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs.

13.54 Is there a process in place to log and review actions performed by emergency Ids associated with the product/ service?

VIOLATION LOGGING MANAGEMENT

13.55 Whether the product/ service is capable of logging the minimum criteria specified to log and report specific security incidents and all attempted violations of system integrity

13.56 Are the product/ service owners aware of their responsibilities with respect to Security incident reporting?

INFORMATION STORAGE AND RETRIEVAL

13.57 Has all the media (file/ floppy/ discs etc) under the control of the product/ service owner been marked with the classification and securely stored with access restricted to authorized personnel only?

13.58 Is there a process in place to ensure that all media under the control of the product/ service owner containing critical information is destroyed in a manner that renders it unusable and unrecoverable?

13.59 Is there a procedure in place that enforces and maintains a clean desk program, which secures all critical information from unauthorized access?

PENETRATION TESTING

13.60 Is it ensured that products/ services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation?

13.61 Is there a penetration test process that ensures whether modifications to the product/ service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted?

13.62 Is there an intrusion detection system in place for all the external IP connections?

14. Maintenance

Maintenance will include the following:

1. Change Request Management and version control
   1.1 Software developed in-house
   1.2 Software purchased from outside vendor
2. Software trouble shooting
3. Backup and recovery
4. Hardware maintenance
5. Training.

Wherever Application Service Provider, who owns the Hardware and maintains the OS/ application software, processes the data for the User, detailed Service Level Agreement should cover entire maintenance.

Change Request Management and Version Control

Software developed in-house

14.1 Check whether requests for changes are initiated by users in a structured change request form (CRF) with pre-printed numbers.

14.2 Are these change requests in warded in a manual/ electronic register with CRF number before initiating the change.

14.3 Are the change requests subjected to feasibility study?

14.4 Verify whether the change request is approved by the Management before effecting the changes in the software and the same is recorded on the CRF.

14.5 Verify whether the changes are made only in the test environment and not in the live environment (separation of test and production libraries).

14.6 After making changes, are they tested adequately before implementation (unit testing, integrated testing, regression testing, etc.)? All these testing procedures should happen only in the test library.

14.7 Once the programs are ready after testing, are they approved by a senior programmer/ Departmental Head? Are such approvals recorded on the CRF?

14.8 After approving the changes, are the changed programs transferred to production library by an independent person who does not have programming/ development responsibilities?

14.9 Does the production library have both sources and executables of the latest version of the programs?

14.10 Check whether the programmers are not given access in the production library. Similarly, check whether the access to the test library is restricted to programmers only.

14.11 Verify if the changes are updated in the user, technical, operations and all other relevant manuals to reflect the current state of the software. Is the CRF updated to this effect?

14.12 Verify if implementation guidelines are prepared by the programmers for properly implementing the changes in the user sites. Are they approved?

14.13 Verify if the changes are implemented at the Users' sites in accordance with the implementation guidelines. Is the CRF updated to this effect?

14.14 After completing all these steps, is the open entry in the change request register rounded off for the relevant CRF number, to bring it to a logical conclusion?

14.15 Is the completed CRF filed along with the system documents?

14.16 Are there procedures to review and monitor all the pending change requests and initiate timely action to resolve the same.

Version Control

14.17 Verify the procedure of roll out of software to the Users sites. Check who is creating the executables from the changed source code for implementation in the user sites? Ensure that such person(s) is/ are independent of development activities.

14.18 Verify if the access to the compilers is restricted to only authorised persons who are empowered to create the executables from the source code.

14.19 Check whether identity of different programs is maintained between any two software release and each release contains all the changes to different programs from the previous release.

14.20 Check whether each release is given a version number.

14.21 Verify if proper records are maintained to reflect the different version numbers of the software, their composition and location. The latest version should be easily differentiated when compared with the older versions.

14.22 If possible, take the latest version of any one program in the test library and arrange to compile the same to arrive at the new exe file. Note down the byte size of the new 'exe' file and compare whether the byte size of the exe program in the live area in the user site is the same as the size noted.

14.23 If multiple User sites are there, verify the control mechanism to ensure whether the same software is being implemented in all such user sites.

14.24 If there are exceptions to certain users, verify if those exception modules of the software are kept in the central control library from where the software is rolled out.

14.25 Verify if there are any register/ database containing the information about which site has which version.

14.26 Check and ensure if backup of all versions of the software are held both onsite and offsite in fire resistant cabinets with proper records.

Software procured from outside vendor

14.27 Verify if there is Annual Maintenance Contract for software and check whether it is currently in force.

14.28 Check if requests for changes are initiated by users in a structured change request form (CRF) with pre-printed numbers.

14.29 Verify if the change request is approved by Management before asking the vendor to effect the changes in the software.

14.30 Are these change requests (CRFs) inwarded in a manual / electronic register before sending it to the vendor for their making changes.

14.31 For all the changes effected and implemented by the vendor, check whether release notes have been provided for all such patches/ releases. If so, does the release notes given by the vendor contain the CRF number submitted by the Bank.

14.32 Check whether the release notes have been circulated to all the users.

14.33 Check whether the open entry in the inward register having the CRF number attended by the vendor is rounded off to reflect the latest pending position.

14.34 Check whether the vendor has updated the user's and operations' manuals to reflect the current state of the software and delivered the same to the Bank.

14.35 Check the procedure for marking off the entries in the inward register for CRFs maintained at CPPD/ IT and ensure whether the current list of outstanding requests are complete and accurate.

14.36 Is there procedure to review and monitor all the pending change requests and initiate timely action to get the same resolved by the vendor in a time-bound manner.

14.37 Verify Service Level Agreement (SLA) with the vendor. Does it lay down the basis of billing, say, based on 'x' number of lines of coding or based on 'y' man hours of effort, etc. Check whether the billing made by the vendor is in accordance with the SLA. Test check whether the billing raised is accurate.

14.38 Does the SLA have penalty clause for delay on the part of the vendor to deliver the changes after submitting the CRF? If so, for any delays on the part of the vendor, does the Bank invoke the penalty clause and charge penalty?

14.39 Verify if any escrow arrangement exists for the source code. If so, check who is the escrow party and inspect their site and check whether a copy of the latest version of the source code is stored there in proper condition with records.

14.40 Check whether one copy of full set of the latest documentation of the software is also kept with the source code in the Escrow's location.

14.41 Check and ensure that Escrow party cannot have unilateral access to the source code and documentation without the knowledge of the software vendor and the Bank.

14.42 Check and ensure if backup of the latest version of the software provided by the vendor is held both onsite and off-site in fire resistant cabinets with proper records.

Software Trouble Shooting

Help Desk

14.43 Check if user calls are logged in a register (manual or electronic) in the Help Desk with a unique identification number for each call. Preferably, the numbering should be serial and unique for each user site.

14.44 Is this number recorded in a Help Desk register in the user's site with nature of the call, date and time of call?

14.45 Does the Help Desk register in the user site reflect all the call identification numbers serially without any missing number in between?

14.46 Is the date and time of resolving the trouble recorded in the Help Desk register? Does it correspond and tally with the records maintained at the Help Desk?

14.47 Are the calls attended to in a timely manner?

14.48 Does Help Desk issue call sheet with solution given duly signed by the user?

14.49 If the troubleshooting is attempted by the Help Desk personnel remotely, check whether any sensitive password was divulged by the user to the Help Desk. This should have been recorded in the Help Desk register both at user site and at Help Desk.

14.50 If sensitive password is revealed to the Help Desk, check the system and application logs and ensure whether the changes made are appropriate to the trouble reported by the user.

14.51 Check whether command log is printed and submitted to the user site, duly signed by the Help Desk official and authenticated by the Help Desk in-charge.

File/ Data Re-organisation

14.52 If the software works on a RDBMS, check whether file/ database re-organisation is carried out at the user site timely to avoid any processing error.

14.53 If any addition to data file/ table space is made, are they approved and in accordance with the software implementation guidelines.

14.54 If operating system/ database fine-tuning is carried out, are they documented in the error log/ Help Desk register.

14.55 As most of these activities require sensitive passwords, does the usage of the same recorded in the password usage register duly signed by the support personnel and user.

14.56 Verify the command logs and ensure that the command and command results are appropriate to file/database re-organisation/ fine tuning, etc.

14.57 Verify if due to OS upgrades any constraint is there in the application software.

14.58 Verify if the interface software is properly tested and implemented if the User is using two or 3applications and data is transmitted through this interface application

Backup and Recovery

Software

14.59 Verify if a latest copy of backup of software (Operating System, RDBMS, application, etc.) is taken and preserved at the user site.

Data

14.60 Verify if different types of data backup are taken periodically at specified intervals as advised by the software developer / vendor.

14.61 Are there proper records for noting the media in which different data backups are stored, data type, location where it is stored, date of backup, due date for recycle, etc.

14.62 Is one copy of data backup kept in an offsite location with proper records?

14.63 Does the database/ system administrator at the user site carry out restoration testing of these backups periodically? Is it recorded and authenticated?

14.64 Are users involved in such restoration testing ?

Purging of Data

14.65 Verify if there is an archival policy and data housekeeping is as per this policy.

14.66 Verify if this archival data can be read as and when required

14.67 Verify if these archival data is stored in safe place.

14.68 Verify if archived data is deleted from the current running system.

14.69 Verify if the printed reports are deleted from the system.

Hardware Maintenance

14.70 Verify if there is any Service Level Agreement between the hardware vendor and CPPD / IT Department.

14.71 Check and ensure that the AMC with the vendor for maintenance of hardware equipments is active and currently in force.

14.72 Verify if the network diagram is available at the user site.

14.73 Does the user site have the names and photographs of the service personnel and are they identified by the users before allowing them to handle the hardware.

14.74 Verify if the hardware inventory is maintained at the user site. Ensure whether the physical stock of hardware items matches with the hardware inventory.

14.75 Verify if the hardware maintenance register is maintained, with full details such as nature of trouble, date and time of reporting, name of the vendor, Engineer's name, date and time of resolution, signature of DBA, signature of Engineer, Initials of Head of the user site.

14.76 Verify if there is a databank of malfunctions of hardware. If so, examine whether similar types of hardware errors are recurring. Check the steps taken by the users/ CPPD/ IT to arrest this trend.

14.77 In case hardware are taken by the vendors for servicing/ repair, does the user site ensure that the equipment does not contain sensitive live data.

Training

14.78 Verify if the Users are given adequate training on the application systems functionalities

14.79 Verify if the Technical persons are given adequate training in the technical details of the application system, to provide necessary troubleshooting / help to users.

14.80 Verify if the Users are aware of the steps to be carried in case of contingency due to non-availability of systems.

15. Internet Banking

Information Systems Security Framework

15.1 Is there a security policy duly approved by the Board of Directors? Is there segregation of duty of Security Officer/Group dealing exclusively with information systems security and Information Technology Division, which actually implements the computer systems? Is the role of an Information Security Officer independent in nature?

15.2 Is the role of an information system auditor independent in nature? (It should be independent of Operations and Technology Unit)

15.3 Bank should ensure that Information Systems Auditor forms part of their Internal Audit Team.

15.4 Bank should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. Bank should review their security infrastructure and security policies regularly and optimise them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.

15.5 Bank should subscribe for the Systems Alerts/Patches. Information Systems Auditor should ensure that all vulnerable patches are applied on a periodic to prevent outsiders exploiting the Bank's systems.

15.6 Under the present legal requirements there is an obligation on Banks to maintain secrecy and confidentiality of customer's accounts. In the Internet banking scenario, the risk of Banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. Does the bank, therefore, institute adequate risk control measures to manage such risks?

15.7 In order to address the risk of liability to customers on account of breach of secrecy, denial of service etc., does the Bank follow a privacy policy?

15.8 Some of the indicated areas, which all Banks need to include as part of the Privacy Policy is given below:

- Banks should safeguard, according to strict standards of security and confidentiality, any information customers share with them.
- Banks will not reveal customer information to any external organization unless they have previously informed the customer in disclosures or agreements, have been authorized by the customer, or are required by law or our regulators.
- Whenever Banks hire other organizations to provide support services, they should require them to conform to our privacy standards and to allow us to audit them for compliance.

Web Server

15.9 Is the web server configured to be a stand-alone unit without any membership to any domain inside the Bank's IT architecture?

15.10 Ensure whether the web server is ported with latest versions of patches and service packs. Specifically, the OS vendor releases patches and service packs with appropriate fixes to prevent Denial of Service attack. These should have been applied to prevent such attacks on the web server.

15.11 All security settings applicable to the operating system in which the web server operates should have been implemented as per IT security policy. Check and ensure this.

15.12 With regard to Super User account :

- Check whether the super user account in the web server is enabled for login only on the system console and not from across the network. Perhaps this is applicable to all user accounts in the web server.
- Check if appropriate parameters are implemented in the operating system of the web server so that the super user account will lock out if too many unsuccessful attempts are made across the network, but remain unlocked at the system console.

15.13 Check if sensitive operating system related executable program files and data files on the web server are not stored on public area but in any other secure location with audit duly enabled.

15.14 IP routing should be disabled in the web server. Check and confirm this.

15.15 Ensure that unauthorized ports for e.g., UDP port No.443 are not allowed inside the web server. Also, ensure that unnecessary services like ftp, messenger, SMTP, telnet, etc. are not installed and active on the web server.

15.16 The facility to shutdown the machine should be restricted to the system console on the web server. Check and ensure this.

15.17 Access to floppy drive, CD-ROM drive, etc. should be restricted in the web server to interactive only to prevent these devices from being shared by all processes on the system. Check and ensure this.

Logs of Activity

15.18 Ensure that auditing is enabled in the web server's operating system and whether the logs are reviewed and authenticated by authorized officials periodically.

15.19 Check if audit trail is enabled on the firewall to log the changes made to the rule base settings and verify whether the logged entries are approved by higher authorities in the IT Department.

15.20 Whether the system administrators are monitoring the logs produced by the Intruder Detection System (IDS) (An intrusion detection system helps in recognizing Security threats and is capable of scanning packets for vulnerabilities. It ensures that distributed denial of service attacks are prevented) and escalating the access violations to the attention of senior management in IT department for guidance. Are these documented and appropriate corrective actions taken?

15.21 Check whether audit trails are enabled for administration activities and whether entries logged in the audit trail are in accordance with process flow chart and no unauthorized activity has been carried out.

De-militarised Zone and Firewall

15.22 Are all Internet connections are routed through a Firewall?

Does a dedicated team manage the Firewall? Are the ports opened only on a "need to have" basis?

15.23 Is there an Intruder Detection System (IDS) implemented?

15.24 Are the application and database servers kept separated from the web server in the demilitarised zone?

15.25 Is the de-militarised zone separated from the Internet cloud by means of a Firewall? (Firewall procurement should be through an approval mechanism, which ensures that only firewalls of highest standards are procured).

15.26 If the de-militarised zone is connected to the Intranet within the Bank, it should be separated by a Firewall. Check and ensure the same.

15.27 Check whether the Firewall rule base is treated as a sensitive information and knowledge of the same is restricted to only authorized officials in the IT/ Computer operations department.

15.28 Ensure that the decision to open specific firewall ports/ rule base is approved in accordance with IT Security Policy (IT Security Policy should list out such ports) e.g. firewalls should block unwanted ports running services such as ftp, telnet, SMTP, etc. into the de-militarised zone. Ideally, only http and https ports are allowable. Check and verify this.

Security Review of all Servers used for Internet Banking

15.29 Carry out a Operating System Security review on all the servers used for internet banking apart from web server as stated in (I) above and ensure that all security parameters have been properly set as per Security Policy.

Database and System Administration

15.30 Has the Bank designated a Database Administrator with clearly defined roles?

15.31 Has the Bank designated System Administrator(s) with clearly defined roles?

15.32 Check whether process flow of administration activities is documented and approved by the Head of Operations and whether the administrators are conversant with the process flow.

15.33 Carry out an application control review of the administration module and ensure whether the functionality as described in the process flow document are adequately met by the module.

15.34 Examine who has access to the Super User account in the administration module?

Examine the procedures for custody and usage of this password and records maintained for the same. Are all usages recorded by the administrator authenticated by appropriate authority.

15.35 Obtain a list of all administrator accounts in the administrator's module and check whether all are attributable to personnel doing the administration job. Extraneous admin IDs should be identified and reported for deletion.

15.36 Check whether the menu options in the admin module are assigned to different administrators on need to know basis, based on functionality offered by the menu options and the work allotment made to the administrator.

15.37 Obtain the list of menu options in the Internet banking module for customers and whether such menu options are assigned to user (customer) IDs only as per their request and as per the policy of the Bank.

15.38 Pay particular attention to user (customer) IDs, which are provided with third party funds transfer facility on the Internet and verify whether they are backed by proper customer request in writing.

15.39 Does the Bank have proper infrastructure and schedules for backing up data? Is the backed-up data periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy? Is Business Continuity ensured by setting up disaster recovery sites? Are these facilities tested periodically?

15.40 Check the procedure for creation of different user accounts for the customers for usage on the internet and whether they are backed by valid customer request for such facility.

Operational Activities

15.41 Considering the legal position prevalent, is it ensured that the Banks not only to establish the identity but also to make enquiry about integrity and reputation of the prospective customer? Therefore, is it ensured that even though request for opening account can be accepted over Internet, accounts are opened only after proper introduction and physical verification of the identity of the customer? Is there a Legal Contract with the customer in place covering the risks of communicating using the Public Network?

15.42 Pay particular attention to customers whose constitution is other than “individual”, particularly corporate accounts and check whether appropriate account opening documentation have been submitted by such customers for internet banking.

15.43 Check if any customer is provided with multiple user IDs, if he/she is not a joint account holder, but only single.

15.44 Any account linkage activity should take place only after ensuring that the user accounts are created based on valid customer requests.

15.45 Check if user-IDs are linked to multiple bank accounts. If so, verify whether such accounts pertain to the same customer only.

15.46 Check the procedure for enabling the customer user ID on the Internet and verify whether adequate precautions are taken by the operations personnel to identify the customer before enabling. Account enablement process should be decided and signed off before product launch. Entire process should be auditable and audit trails should be enabled for the same (Each Bank can decide whether they can pre-enable or post-enable the user accounts based on their policy).

15.47 Check the procedure for creation of new password for customers who report having forgotten the password. Verify the procedure for ensuring the identity of the customer before creating the new password.

15.48 Verify whether adequate records (either electronic or manual) are maintained for the customer user IDs created, enabled, new passwords provided, etc. and whether they are authentic. Test check the instances of change of customer's passwords and whether they are backed by valid customer requests.

15.49 Do all applications of banks have proper record keeping facilities for legal purposes? It may be necessary to keep all received and sent messages both encrypted

Application Control Review of Internet Banking Application

15.50 Does the software allow creation of user-IDs in the same name more than once?

15.51 Does the software encrypt the passwords one way and store the same in encrypted form in the database?

15.52 Does the software display the password as it is keyed in? (It should not be displayed on the screen).

15.53 Does the software lock the user-ID if it is used for X unsuccessful times to logon to the system?

15.54 Does the software force the User to change the password at set periodical intervals?

15.55 Does the software maintain password history i.e., the same password should not be used again on rotation basis.

15.56 Check whether the software logs the instances of change of user's (customer's) password in the audit trail?

15.57 Does the software allow automatic logical deletion of inactive user IDs after certain period of time?

15.58 Does the system maintain password length to be of minimum 6 or 8 characters or as the case may be with combinations of alpha, numeric and special characters?

15.59 Check whether the menu options available on the web page for a customer after logging on to the system provide only appropriate functionality as designed and no deviation is possible.

Application Security

15.60 Is the Security infrastructure properly tested before using the systems and applications for normal operations? Following needs to be taken care of for ensuring that Security infrastructure is tested properly before using the systems and applications:

- As part of the System Development Life Cycle (SDLC), during the development stage an Information Security Review needs to be conducted covering the entire system and architecture review
- Comprehensive Information Security related checks needs to be conducted during the Coding & Testing stage
- On completion of User Acceptance testing (UAT), all Internet related systems or applications needs to be penetration tested by an independent party.
- Banks should enter into an Agreement with the independent party who conducts the penetration testing covering both Legal and Contractual terms.

15.61 Following should be covered as part of penetration tests/ vulnerability tests:

1. Check for following common vulnerabilities:
   - IP Spoofing
   - Buffer overflows
   - Session hijacks
   - Account spoofing
   - Frame spoofing
   - D-DoS attacks
   - Caching of web pages
   - Cross-site scripting
   - Cookie handling.

2. As per RBI's guidelines PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. Since Government & RBI is in the process of identifying a PKI service provider, it may take some time to implement PKI in all the Banks. However, as it is not yet commonly available, does the bank use the following alternative system during the transition, until the PKI is put in place:
   - A static ID and password login process.
   - Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the Banks themselves using a Certificate Server.
   - The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data likes passwords in transit within the enterprise itself.