Information systems audit policy for the banking and financial sector

Working group for information systems security for the banking and financial sector

Department of Information Technology
Reserve Bank Of India
Mumbai
October, 2001

FOREWORD

The business operations in the banking and financial sector have been increasingly dependent on the computerised information systems over the years. It has now become impossible to separate Information Technology (IT) from the business of the banks and the financial institutions. There is a need for focussed attention on the issues of the corporate governance of the information systems in computerized environment and the security controls to safeguard information and information systems.

The application of Information Technology has brought about significant changes in the way the institutions in the banking and financial sector process and store data and this sector is now poised to countenance various developments such as Internet banking, e-money, e-cheque, e-commerce etc., as the most modern methods of delivery of services to the customers. The telecommunication networks have played a catalytic role in the expansion and integration of the Information Systems (IS), within and between the institutions, facilitating data accessibility to different users. In view of the critical importance of IS, there is a need to exercise constant vigilance for the safety of the financial systems. Structured, well defined and documented security policies, standards and guidelines lay the foundation for good IS security and each institution is required to define, document, communicate, implement and audit IS Security to ensure the confidentiality, integrity, authenticity and timely availability of information, which is of paramount importance to business operations.

Reserve Bank of India constituted a 'Working Group for Information Systems Security for the Banking and Financial Sector' to discuss and finalise the standards and procedures for IS Audit and IS Security Guidelines for the banking and financial Sector. The Working Group has prepared this report on the 'Information Systems Audit Policy' including 'Information Systems Security Guidelines'.

This report discusses various aspects of IS Audit such as the objectives, approaches, methodology, charter, planning, standards and guidelines, sampling, evidence and documentation. It discusses the skills, the IS auditors will require to possess as also the way they will require to address the irregularities, observed

 during auditing. It discusses the issues relating to the corporate governance of Information Systems and Security Controls. It has brought out the primary roles to be performed by the Auditor and the Auditee.

Under the 'Information Systems Security Guidelines', the report discusses IS Security Controls relating to computer hardware, software, network, Telecommuting/Tele-working, Mobile Computing, Computer Media Handling, Voice, Telephone and related equipment and Internet and the procedures/methodologies to be adopted to safeguard information and information systems. It discusses issues such as Change Control Mechanism, Separation of Development and (Production) Operational Facilities, Information Handling and Back-up, Electronic Mail and Financial Services/Products. It emphasises the use/implementation of Firewall, Digital Signature, Cryptographic Controls, Business Continuity Planning (BCP), Framework/Disaster Recovery Planning (DRP) including Cryptographic Disasters. It also discusses various other issues relating to Certification Authorities (CAs)/Trusted Third Parties (TTPs), Compliance with Legal Requirements, Intellectual Property Rights (IPR), Review of IS Security Policy and Human Resources.

The IS Audit Policy issues and the IS Security Guidelines, discussed in this report, are indicative ones only and each institution will require to examine the adequacy of the security controls on an on-going basis and enhance the same, as required, from time to time. We are forwarding a copy of this report for information and comments. We request all the banks and the financial institutions to set up appropriate audit and security systems in this vital sector.

The Chairman, Members of the Working Group and the officials of the Department of Information Technology, Reserve Bank of India, Mumbai, associated with the preparation of this report, deserve compliments for the good work done.

(Vepa Kamesam)
Deputy Governor

Mumbai 6-11-2001

CHAPTER 1
Introduction

1.1 The developments in Information Technology have a tremendous impact on auditing. Information Technology has facilitated re-engineering of the traditional business processes to ensure efficient operations and improved communication within the organisation and between the organisations and its customers. Auditing in a computerized and networked environment is still at its nascent stage in India and established practices and procedures are evolving. Well planned and structured audit is essential for risk management and monitoring and control of Information Systems in any organisation.

Information Systems (IS) auditing is a systematic independent examination of the information systems and the environment to ascertain whether the objectives, set out to be met, have been achieved. Auditing is also described as a continuous search for compliance. The Auditors may not necessarily examine the entire system. They may examine a part or parts of it only. Auditing covers primarily the following broad major areas of activity :

a) gathering of information

b) comparison of information and

c) asking why

1.2 Types of Audit : Various methods are adopted for categorizing Audit . One such method of categorization divides audit into two types e.g. **Adequacy Audit** (also called **Systems Audit**) and **Compliance Audit**. Another method categorizes Audit by levels – **Internal Audit**, **External Audit** and **Extrinsic Audit**. Yet another method of categorization is by parties – First Party, Second Party and Third Party audits. The most common types of audit are **Financial Audit, Compliance Audit, Information Systems Audit and Operations Audit.**

1.3 Banking & Financial Activities and Risks : The deployment of Information Technology in banks and financial institutions, both in the front and back office operations, has facilitated greater systemic efficiency in the banking and financial sector. It has, at the same time, introduced new areas of risk. Risk is inherent in the traditional banking and financial activities. However, risk in a computerized and networked environment is multifarious such as **operational risk, reputational risk, legal risk, credit risk, liquidity risk, interest rate risk, foreign exchange risk** etc., as briefly discussed hereunder :

1.3.1 Operational risk arises out of the problems concerning the reliability and integrity of the Information Systems. The extent of such risks depends on the security features, design

and implementation of security policies and procedures, adopted in an electronic banking system. Network security, database security, data integrity, appropriateness of the security policies and practices and the likely misuse of the information and information resources by the employees, customers and third parties are some of the factors, which require to be addressed for risk measurement in a computerized and networked environment in the banking and financial sector.

1.3.2 Reputational risk is very closely intertwined with the other kinds of risks. Failures, frauds, lack of proper delivery or non-delivery of information to customers, monetary loss to customers, lack of personal touch and litigation are some of the factors which cause loss of reputation to an organisation. Lack of reputation is a very serious problem for any business and the banking/ financial institution is no exception. Lack of reputation is usually due to serious security loopholes and lapses in the information systems, lack of fast and efficient delivery channels for retail banking and financial services and the market's general lack of trust in electronic banking/financial channel, say credit cards, which constitutes one type of electronic money or e-cash or plastic money. The occurrence of external and internal attacks on an organisation's information and Information Systems may cause serious damage to public confidence in the organisation.

1.3.3 Legal risk emanates from various factors such as the lack of adequate legal framework, inappropriate, ineffective, irrelevant and inapplicable Information Technology Act, inappropriate customer secrecy obligations on the part of the banks and financial institutions, inadequate privacy policy for the customers, Certification Authority risk, Trans-border financial transactions with very little or no legal backing or international law for the same, lack of legal provisions for public trans-border communication network such as Internet, other private networks etc.

1.3.4 Credit risk arises when the parties default in repayment of loans and advances. In computerized environment, credit risk gets enhanced because credit is channelised through electronic channels, which transgress the barriers of time and space. Credit appraisal in order to ascertain the credit worthiness of a prospective customer is difficult to verify as multiple remote customers may access the bank round the clock for credit through non-traditional channels of communication with little or no ways and means being available with the banks to completely ascertain the veracity of their claims within the set limits of response time, as per the guidelines for Customer Relationship Management. In cases of credit flow through trusted third parties like the operators of electronic inter-bank/institutional payment gateways, any default on the part of the third party operators in assessing the credit worthiness of the final customers would boomerang on the bank and has to be considered as another factor contributing to credit risk. Credit risk assumes great importance in an electronic banking environment.

1.3.5 Liquidity risk arises when an entity fails to meet its payment obligations in a timely manner. Banks, which may provide the facility of electronic money, shall be liable to arrange for adequate funds in case of redemption or settlement on electronic money. Any default could lead to legal wrangles and loss of liquidity.

1.3.6 Interest Rate risk arises due to variation in the interest rates. In case of banks offering electronic money, any fluctuation in the interest rate, which affects the value of the assets, created by electronic money, are liable to create interest rate risk liability on the bank.

1.3.7 Cross-border Transactions Risks: Electronic banking envisages a borderless world of financial services and therefore, risks, arising out of variation in the exchange rate, are likely to create additional risks for a bank. Different exchange rates, existing in different countries, mean that the banks need to analyse not only the exchange rate fluctuations with respect to the currencies of their respective countries, but exchange rate fluctuations between two or more (other) countries also. This kind of risk is likely to arise in case the bank has to cover losses due to unfavourable exchange rate fluctuations or in case, the third country participants in an electronic payment system are unable to fulfill their financial obligations due to social, economic and political factors in their respective countries.

1.4 Risks accentuate the need for comprehensive audit, as under, in a computerised environment:

1.4.1 Financial Audit :

A financial audit is an examination of an organization's financial statements. A financial audit like other types of audit has to be conducted by an independent auditor. Auditors must not only be independent, but have to also appear to be independent.

The term audit here describes the investigation, which the auditors undertake to provide the basis for their analysis and opinion/suggestion. As a part of financial audit, auditors consider and evaluate the internal controls, put in place by an organization, in regard to the preparation of the financial statements. This evaluation gives them a feel of the accuracy and reliability of the information in the organization's accounting system. The auditors gather evidence/information to substantiate every material item appearing in the financial statements. Auditors also build up procedures, designed to determine that the financial statements and the accompanying notes are complete in all respects.

After completing the audit, the auditors express their expert opinion as to the fairness of the financial statements. These opinions are expressed in the form of audit reports. Audit reports, however, do not guarantee the accuracy of the financial statements, but provide the auditor's professional opinion only on the overall fairness and accuracy of the financial statements, based on the information made available to the Auditors.

The primary purpose of financial audit is to determine the overall accuracy and fairness of the financial statements and not to detect any or all acts of fraud. Most audit procedures are based on samples and therefore, it may not be possible for the auditors to verify all the transactions. However, frauds, which render the financial statements misleading, require to be brought under the scope of any form of audit. Auditors design their investigation to detect errors and omissions that are material to the financial statements. With respect to the financial statements, an item is material, if knowledge of the item might reasonably be expected to influence the decisions of the users of the financial statements.

1.4.1.1 Financial Audit in Computerized Environment for the Banking & Financial Sector :

The use of Information Technology has revolutionised the banking and financial sector. The manner in which the financial services are being offered by the banks and the financial institutions is undergoing a sea change. A set of new financial services such as Electronic Banking, Tele-banking, Electronic Clearing Systems, Electronic Funds Transfer, Electronic Money, Smart Cards, Credit Cards etc. is fast gaining ground. Information Technology has helped the banks and the financial institutions to build up more efficient back-office systems togetherwith automated management information systems for asset-liability management and risk analysis.

In a computerized environment, the financial statements could be generated from diverse database systems, operating on different operating systems. The financial transactions, on the basis of which the financial statements are generated, could be fully automated and there may or may not be proper audit trails, time stamps like log reports and the like to monitor and trace these transactions. Further, these transactions may not be bound by the traditional boundaries of time, space and even organizations. Various legs of a transaction could have been effected not only at different points of time, but at geographically different locations and between different banks or financial institutions. Needless to say that such transactions become very complex.

An organisation's financial statements reflect a set of management assertions about its financial health. The task of an auditor is to determine whether the financial statements have been fairly presented. To accomplish this, the auditor has to establish the audit objectives, design procedures and gather evidence/ information, which may corroborate or refute the management's assertions.

1.4.1.2 In a computerized environment, financial audit requires to be carried out in three phases, as under :

In the first phase, an audit plan has to be drawn up. This will require to be done by reviewing the organisation's policies and practices, regulatory and legal controls as applicable, trade practices and conventions and internal control mechanism. The financially significant applications and the controls over the primary transactions, which are processed by these applications are also studied in this phase of audit. The techniques for gathering the desired information at this phase include questionnaires, interviewing management/concerned authorities and reviewing the systems documentation.

In the second phase, the internal controls, which have been set up, are tested. Various tests are conducted to test the ruggedness of the internal controls.

In the third phase, detailed drill-down tests are conducted by scrutiny of the individual transactions, selected from a fairly large sample of the business transactions.

1.4.2 Compliance Audit :

An organization's operations are subject to a variety of laws and regulations. Violation of

these laws and regulations would result in imposition of huge fines and penalties. Compliance with these laws and regulations is monitored by the regulatory authorities through Compliance Audit.

Compliance Audit of the computerised transactions is a difficult and complicated task. There has to be a systematic examination of the transactions, at least a reasonable sample thereof, to understand the various issues involved. Let us take an example of a simple money transfer, say electronic funds transfer, from the account of a customer of a bank in one country to the account of a customer in another bank of another country. In this case, the compliance with the foreign exchange management laws of the two countries, regulatory guidelines, issued by the Central Banks and the taxation laws of the two countries, to name a few of the compliance requirements, will require to be examined. Further, what kind of accounting procedure has been followed for effecting debit and credit on the customer accounts and the issue of advices will require to be examined. Whether such money transfer amounts to money laundering in any way or any other financial irregularity will require to be examined. A complex maze of laws, regulations and audit rules will require to be considered under Compliance Audit. Any version change or change of application and data migration should be subject to Audit.

Compliance Audit follows a three-phase-audit route. Compliance with various statutory guidelines, legal and regulatory guidelines and adherence to trade practices and conventions require to be thoroughly tested under Compliance Audit.

In the planning phase or the first phase of Compliance Audit, the various applicable rules, regulations, laws, regulatory fiats etc. will require to be studied and noted down. Appropriate tests, which may verify compliance with these rules, regulations, laws and regulatory fiats, will require to be decided and planned.

In the test/control phase or the second phase of Compliance Audit, the tests, as planned in the first phase, will require to be carried out and the compliance therewith observed. Variations/exceptions/violations will require to be noted down for mention in the audit report.

In the last phase of Compliance Audit, a sample of transactions is tested in detail for compliance.

Compliance Audit is conducted in the banking and financial organisations to ascertain whether various rules and regulations, as laid down by the regulatory authorities such as the Central Bank, Capital Market Regulator, Exchange Control Regulator etc., have been complied with.

1.4.3 Information Systems (IS) Audit :

IS audit is a systematic process of objectively obtaining and evaluating evidence/ information regarding the proper implementation, operation and control of information and the Information System resources. IS audit could be considered a part of Financial Audit. The lack of physical procedures, which can be easily verified and evaluated, injects a high

degree of complexity into IS audit. Therefore, a logical framework for conducting an audit in the IT environment is critical to help the auditor identify all important processes and data files.

IS audit follows a three-phase process, as applicable to Financial Audit and Compliance Audit. The first phase is the audit planning phase, followed by the test of controls phase and finally, the substantive testing phase.

In the planning or first phase, an IS auditor must identify the various risks and exposures and the security controls, which provide safeguards against these exposures. The tests, which need to be conducted to make the second phase of the audit effective, are also planned in detail in the first phase.

In the second phase, the security controls are tested. Control activities in an organization are the policies and procedures used to ensure that appropriate actions are taken to deal with the organisation's identified risks. One of the primary areas of IS audit is to check the effectiveness of these security controls. Control activities, in turn, are divided into two major areas – **Computer Controls and Physical Controls.**

Within Computer Controls and the security controls are the general controls and the application controls. General controls pertain to area-wise concerns such as controls over the data center, organizational databases, systems development and program maintenance. Application controls ensure the integrity of specific application software. Physical Controls include access control, transaction authorization, segregation of duties, supervision, accounting records and independent verification.

In the third or the Substantive Testing Phase, individual transactions are tested. The IS audit substantive tests extensively use computer assisted audit tools and techniques. Audit of Information Systems is a very challenging job, specially in the light of the fast changing pace of Information Technology including Communication Systems.

1.4.4 Information Systems Audit for the Banking & Financial Sector:

Audit is one of the major controls for monitoring management activities in the banks and financial institutions. In a computerized environment, IS audit is a very effective and necessary activity. Usually the IT implementation in the banking and financial organizations is done by adopting a mix of different methodologies – **internal development and deployment and third party product development and deployment.**
In case of internally developed and deployed IT systems, IS audit will require to be done by a team of specially trained internal or external auditors. However, it is preferable to have the IS audit conducted with the help of suitable external agencies with the required skills and expertise to ensure independent nature of audit.

In case of development and deployment of the IT systems by third parties, the IS audit requires to be conducted by trusted auditor/s with skills and expertise, required for the purpose. IS audit assumes greater significance because a large number of critical and strategic financial operations in the banking and financial sector are wholly or partly being

handled by the computerized systems.

1.4.4.1 Information Systems Audit & Computer Aided Audit Tools & Techniques:
With the help of computer aided audit tools and techniques, an IS audit becomes more scientific and meaningful. There are five basic approaches, as under, for testing the application controls using CAATT (Computer Aided Audit Tools and Techniques).

a) Test Data Method – This method is used to establish application integrity by processing specially prepared sets of input data. The results of each test are compared with the pre-determined expected results. The auditor first obtains the current version of the application and then generates the test transaction files and test master files. Thereafter, the test transaction files are input into the program and the result in the form of routine output reports, transaction listing and error reports are collected.

Further, updated master files are also checked for correct/expected outputs. The test results are compared with the expected results, either manually or again through a computer program.

b) Base Case System Evaluation – Under this method, a base test set of transactions is prepared along with the expected results. This set of transactions is comprehensive and all possible transaction types are included. Whenever testing is done, the results are compared with the results of the base test data results, which were obtained initially.

c) Tracing – Under this method, the test data does a virtual walk through the application logic. The application under review must undergo a special compilation to activate a trace option. The test data, prepared for tracing, is run and the result shows the exact listing of the programmed instructions, executed while the test data was processed.

d) Integrated Test Facility – This is an automated test technique, where the audit module is designed in the application program itself to be run in the normal course of operations by the application program with a specific choice of test data and where the application program distinguishes between the actual transactional data and test transactional data for simultaneous integrated audit and normal operations.

e) Parallel Simulation – This requires the auditor to write a program that simulates the key features and processes of the application. The program is run on the pre-processed actual transactional data and the results obtained are compared with the actual results obtained.

1.4.4.2 For the purpose of **Concurrent Audit or Real Time Audit**, sometimes an embedded audit module is used to identify important transactions, while they are being processed and copies of such transactions are extracted in real time. Threshold levels and pre-defined conditions are set and all transactions, which cross the threshold or meet the conditions, are segregated and copies thereof audited in real time.

1.4.4.3 Database Auditing is another area of interest for the IS auditors. Data structures vary from flat files to relational database structures. In order to effectively audit

databases, a process of data normalization is essential. Database normalization is a technical matter and is usually the responsibility of the Systems Professionals. However, technical knowledge of the same is essential for the IS auditors also. The IS auditors, while performing the software audit, should ensure from the system documents that the database is properly normalized and there is not much redundancies and dependencies, as poorly normalized database could affect the integrity of data. The database constraints will also require to properly examined.

1.4.4.4 With the advent of Corporate Networks, Payment Gateways and new products like Internet Banking, Anywhere Anytime Banking etc., which primarily rely on various public and private networks for their operation, Network Audit forms a key area of IS audit. Network Audit covers all aspects of the network, right from the communication channels, network equipment like switches, bridges, routers, firewalls to internetworking issues and security controls. To ensure continuous adequacy of security controls in networked environment, each organisation will require to regularly conduct penetration testing in respect of the Information Systems with the help of third parties under well specified terms and conditions, agreed therefor with such third parties.

1.4.5 Operations Audit :

Operations Audit is mostly considered part and parcel of the other types of audit.

1.5 Audit for the Banking & Financial Sector in Computerised Environment and Regulator's Role :

A number of regulators regulate the activities in the banking and financial sector. In an ideal situation, each financial market like the call money market, term money market, securities/debt market, capital market, foreign exchange market, derivatives market and commodities market should have independent statutory regulators. However, in most of the countries, more often than not, both the regulatory and supervisory powers rest with the same independent statutory regulatory authority.

The job of the regulator is to ensure the soundness of the financial markets and the financial systems and to work towards their growth. As a part of the regulator's mandate, various regulations in the form of guidelines, circulars and instructions are issued to the participants in the financial markets from time to time. These guidelines relate to the macro and micro levels. The mandate of the regulator for supervision encompasses the functions of audit. **The audit is done to ensure systemic efficiency, efficacy, speed and to prevent frauds.**

In case of various kinds of audit in a computerized environment, the regulator will require to issue from time to time, the guidelines, concerning the level of transparency and access to the financial statements, information and information systems. For the specific purpose of audit, the entities in the banking and financial sector will require to adhere to standard practices and policies regarding the development and deployment of computer resources. These guidelines will specify not only the key areas of statutory audit, but will also include the areas of operation, where concurrent audit may be necessary. Further, areas will require to be identified for off-site and on-site inspection and audit by the regulator.

For this purpose, a set of standards, practices and procedures will require to be worked out for adoption by each organization in the banking and financial sector regarding each and every aspect of computerization including, among others, networking, applications, databases, security features, audit and accounting features. The standards will require to be generic, open and minimal. These standards, practices and procedures will ensure that the banks and financial institutions can be inspected and audited in a more comprehensive and elaborate manner, keeping in view the basic principles in which the computers, networks, databases, applications and security provisions operate in a computerized environment.

The guidelines will require to provide for sufficient safeguards to be built in the Information Systems to ensure systemic ruggedness to reduce the risk of cyber and digital crimes like hacking, spamming, unauthorised access and destruction or manipulation of the information and the information systems.

The regulator may have to initially take the help of trusted and independent third party Information Systems Auditors, with suitable skills and expertise for the purpose, alongwith its personnel, for auditing inter-institutional applications. The regulator will require to develop a team of expert Information System Auditors in-house for the purpose. Adequate importance will require to be given to security features in the Information Systems such as the use of digital certificates, digital signature, encryption, time stamping and audit trails. These security controls will require to be implemented by the entities in the banking and financial sector only after careful selection and regular audit by trusted independent third party/ ies, well-versed in the latest technology for the same.

The regulator has also to ensure that all kinds of financial risks like operational risks, credit risks, interest rate risks etc. are managed by the banks and the financial institutions through comprehensive and effective means of off-site, on-site and concurrent audit and inspection. This assumes much more significance in an environment, where the speed of financial transactions is very high with much larger ramifications. Better accounting norms, income recognition norms, stricter capital adequacy measures etc. will require to be devised and implemented.

1.6 IS audit and Certified Information Systems Auditor (CISA)/ Certified Information Systems Security Professional (CISSP):

The core function of the banks and the financial institutions is to provide banking and financial services and not Information Technology related services. These organisations may not have the necessary skills and expertise to conduct IS audit on their own. Further, these organisations may procure various third party security products for use in their Information Systems. These security products will require to be IS audited and vetted before deployment as also subsequently, at regular intervals. IS audit is a very specialised task and will require to be carried out by suitably qualified and skilled personnel, prefarably by external agency/ies in association with suitable in-house personnel initially. Therefore, these organisations will require to use Certified Information Systems Auditors (CISA), Certified Information System Security Professionals (CISSP) etc. for conduct of IS audit in their respective organisations. However, they will require to expeditiously develop

necessary in-house skills and expertise for the purpose.

1.7 The RBI constituted a 'Working Group for Information Systems Security for the Banking and Financial Sector', under the Chairmanship of Executive Director Dr.R.B.Barman and with representation from a few major banks in the Public and Private sectors and a few institutions in the private sector, engaged in Information Systems Audit work, vide the then Deputy Governor Shri S.P.Talwar's memorandum dated the 18th May, 2001, to discuss and finalise the standards and procedures for Information Systems Audit and Information Systems Security guidelines for the banking and financial Sector.

1.7.1 The Working Group met on three occasions i.e. May 31, 2001, October 12, 2001 and October 19, 2001. The two reports on Information Systems Audit Policy and Information Systems Security Guidelines were discussed and finalised in the 3rd meeting of the Working Group, held on October 19, 2001. As the Information Systems Audit has to be performed primarily on the Information Systems Security Controls, the Working Group decided that the report on the 'Information Systems Security Guidelines' should appear as an annexure to the report on the 'Information Systems Audit Policy'.

1.7.2 The 'Working Group on Information Systems Security for the Banking and Financial Sector" recommends that the 'Information Systems Audit Policy' needs to be read with the "Information Systems Security Guidelines" (ANNEXURE) to provide a reasonable measure of totality to the approach to Information Systems Audit and Information Systems Security, to be adopted by the organisations in the banking and financial sector in the country.

1.7.3 Information Systems Audit is a challenging job in an increasingly automated world of financial services. Auditing is a never ending exercise and in fact, it is a perpetual quest for compliance. This document contains some policy issues/guidelines on the standards, practices and procedures for the conduct of Information Systems Audit, to be adopted by the organisations in the banking and financial sector.

1.7.4 The members of the Working Group sincerely acknowledge the contributions made by Dr. A.M. Pedgaonkar, General Manager, Department of Information Technology and Shri S.N. Panda, Assistant General Manager, Department of Information Technology in preparing the draft chapters and the secretarial help provided by Shri L. Ponnudurai, Manager and Smt. Ananthalakshmi Raman, Assistant Manager. Shri Panda has worked really hard in the preparation of the draft chapters after going through vast literature on the subject from national and international sources. The members sincerely appreciate Shri Panda's efforts.

CHAPTER 2
Executive Summary

2.1 High profile problems, experienced by a variety of organizations in recent years, including the organizations in the banking and financial sector, have focussed attention on

the issues relating to the corporate governance of the information systems. It is the management's responsibility to safeguard all the assets of the organisation. To discharge this responsibility as also to achieve its expectations, the management must establish an adequate system of internal controls. The formal means by which the management discharges its responsibility to establish an effective system of internal controls over an organisation's operational and financial activities is now subject to increasing public scrutiny and often forms part of the scope of audit for both the internal and the external auditors. During the course of IS audit, the Information Systems Auditor has to obtain sufficient, reliable, relevant and useful information to achieve the audit objectives effectively. The audit findings and conclusions will require to be supported by appropriate analysis and interpretation of this information.

2.2 Reporting on corporate governance of the information systems will involve auditing at the highest level in the organisation and may cross divisional, functional or departmental boundaries. The management/designated authority in the organization will have to, therefore, ensure that the audit charter or the engagement letter for the IS auditor clearly states that the scope of IS audit includes the corporate governance of the information systems and technology togetherwith the reporting line to be used, where corporate governance issues are identified.

2.3 Each organization is required to make available the following information on the corporate governance structure to the IS auditor :
a) Member(s) of staff with responsibility of the information systems.
b) Information, received by such member(s) of staff, to enable them to discharge their responsibilities.
c) Framework of control, adopted by the management of the organization, in policy setting. Policies, approved by the Board of

Directors of the organization, to direct the use and protection of the information and the information systems.

2.4 Audit Objectives :
The objectives of an audit of the corporate governance of information systems may be affected by the intended audience's needs, the level of dissemination intended and the national and industry regulations. The IS auditor will require to consider the following options, while establishing the overall objectives of the audit. The IS audit objectives for the audit of the corporate governance of the information systems will usually depend upon the framework of internal control exercised by the management.
(a) Reporting on the system of governance of the information systems

(b) Reporting on both the system of governance and its effectiveness

(c) Inclusion or exclusion of the financial information systems

(d) Inclusion or exclusion of the non-financial information systems

2.5 Scope of Audit :
The IS auditor will require to include in the scope of the audit the relevant processes for

planning and organising the information systems activity and the processes for monitoring that activity. The scope of the audit will also include the internal control system(s) for the use and protection of the information and the Information Systems, as under :
a) Data

b) Application systems

c) Technology

d) Facilities

e) People

2.6 Performance of Audit Work :
The IS auditor should review the following :

a) Minutes of the meetings of the Board of Directors for audit information relating to the consideration of the matters concerning the information systems and their control and the supporting materials for any such items.

b) Minutes of the meetings of the Audit Committee reporting to the Board of Directors for audit information relating to the consideration of the matters concerning the information systems and their control and the supporting materials for any such items.

The IS auditor will require to consider whether the information obtained from the above reviews indicates coverage of the appropriate areas. The various issues / documents / statements / areas, among others, which the IS auditor will require to examine include as under :
a) IS mission statement and agreed goals and objectives for information systems activities.
b) Assessment of the risks associated with the organisation's use of the information systems and approach to managing those risks.
c) IS strategy, plans to implement the strategy and monitoring of progress against those plans.
d) IS budgets and monitoring of variances.
e) High level policies for IS use and the protection and monitoring of compliance with these policies.
f) Major contract approval and monitoring of supplier's performance.
g) Monitoring of performance against service level agreements.
h) Acquisition of major systems and decisions on implementation.
i) Impact of external influences on IS such as Internet, merger of suppliers or liquidation etc.
j) Control of self-assessment reports, internal and external audit reports, quality assurance reports or other reports on IS.
k) Business Continuity Planning, Testing thereof and Test results.
l) Compliance with legal and regulatory requirements.
m) Appointment, Performance Monitoring and Succession Planning for senior IS staff including internal IS audit Management and Business Process Owners.

2.7 Review of Policies and Compliance :

The IS auditor will require to consider whether the policies issued cover all of the appropriate areas for which board-level direction is necessary in order to provide reasonable assurance that the business objectives are met. Such policies on board level direction will require to be documented ones only and such documented policies shall, among others, include the following :

a) Security Policy

b) Human Resources Policy

c) Data Ownership Policy

d) End-user Computing Policy

e) Copyright Policy

f) Data Retention Policy

g) System Acquisition and Implementation Policy

h) Outsourcing Policy

2.8 The IS auditor will require to assess whether the policies issued are appropriate to the information system needs/requirements of the organisation. Further, the IS auditor will require to assess whether the policies are being adequately enforced, including the communication of the policies, existence and awareness of standards, procedures and methodologies to support the policies, allocation of the responsibility for enforcing the policies and the system, put in place by the organization, to monitor and report on the compliance with the policies.

2.9 Responsibilities of the Owner of the Business Process :

The IS auditor will require to review the responsibilities of the business process owners, as under and assess whether these are appropriate to support the policies set at the Board of Director's level.

a) Assessment of whether the business process owners have the skills, experience and resources necessary to fulfill this role.

b) Review of the information received by the business process owners and to assess whether it is appropriate to enable them to discharge their responsibilities and to monitor compliance with the policies.

Information that may be considered appropriate includes as under:

i) Reports of attempted access to the systems supporting business processes and follow-up action taken.

ii) Reports of changes to user access rights, including new users and those whose access rights have been removed.

iii) Reports of the results of business continuity tests and follow-up action taken.

iv) Reports on the results of feasibility studies and tendering processes for systems acquisition.

v) Reports of the results of user acceptance testing of new systems or changes to the

existing systems.
vi) Reports on performance against agreed service levels.
vii) Statistics on the availability, number of failures, number of system changes requested and implemented etc.
viii) Status of system changes in progress.
ix) Reports of changes to corporate data dictionary entries.

c) Assessment of the system which produces the above information and its reliability, integrity and potential for management override.
d) Where the organisation has internal audit resources, which is an important element of the corporate governance process, assessment whether the appropriate level of the involvement of the internal audit resources has been provided.

2.10 Consideration of External Factors :

Corporate governance of the information systems involves directing as well as controlling. The industry in which the organisation operates, trends in the IS industry and the social and political changes may influence the benefits, which the organisation can obtain from the use of the information systems. The IS auditor will require to verify that the organization has put in place the procedures to monitor the external factors, which are relevant to the organization. The IS auditor will require to also verify whether the material issues, which require all computerised organisations to assess their potential effects well in advance, current at the time of the audit exercise, are under active consideration at the appropriate level. The organisation has to plan appropriate actions to avoid the potential material adverse effects of such issues. In case such issues are not being actively considered at the appropriate level in the organisation, the IS auditor will require to promptly report this matter to the designated authority/ies in the organisation.

2.11 IS Specialist Staff :

The IS auditor will require to consider the position or functions of the IS specialist staff in the organisation and assess whether this is appropriate to enable the organisation to make the best use of IS to achieve its business objectives. The control of the information systems, even in decentralised and end-user run environments, should include segregation of conflicting duties. The IS auditor will require to assess whether the management of the IS specialists and the non-specialists with IS responsibilities is adequate to address the risks to the organisation from the errors, omissions, irregularities or illegal acts.

2.12 Reporting :

The IS auditor will require to address reports on the corporate governance of the information systems to the Audit Committee/Board of Directors or any other designated authority in the organisation. In case of detection/identification of failures in corporate governance, the same will require to be urgently reported to the designated authority in the organisation. The IS audit report on corporate governance of information systems should, among others, include the following :

a) A statement that the Board of Directors is responsible for the organisation's Information Systems and formulation and implementation of the system of internal controls.

b) A statement that a system of internal controls can only provide reasonable and not absolute assurance against material misstatement or loss.
c) A description of the key procedures, which the Board of Directors has approved/established, to provide effective internal control and the related supporting documentation presented to the Board of Directors.
d) Information on any non-compliance with the national or industry codes of practice for corporate governance.
e) Information on any major uncontrolled risks.
f) Information on any ineffective or inefficient control structures or control measures togetherwith the IS auditor's recommendations for improvement.
g) The IS auditor's overall conclusion on the corporate governance of the information systems, as defined in the scope of audit.

2.13 Follow-up Activities :

The weaknesses, if any, in the system of corporate governance of information and information systems can cause wide ranging and high risk effects in the organisation. The IS auditor will require to, therefore, where appropriate, carry out sufficient, timely follow-up work to verify that the management action is taken promptly to address such weaknesses.

CHAPTER 3

Objectives of Information Systems Audit

3.1 The objectives of IS audit are to identify the risks that an organisation is exposed to in the computerized environment. IS audit evaluates the adequacy of the security controls and informs the Management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise in an organisation. The overall objectives of the normal audit exercise do not change, when applied to the computerized environment. The major objectives of IS audit include, among others, the following:

a) Safeguarding of Information System Assets/Resources

b) Maintenance of Data Integrity

c) Maintenance of System Effectiveness

d) Ensuring System Efficiency

3.1.1 Safeguarding of Information System Assets/Resources :

The Information System Assets of the organisation must be protected by a system of internal controls. It includes protection of hardware, software, facilities, people (knowledge), data files, system documentation and supplies. This is because hardware can be damaged maliciously, software and data files can be stolen, deleted or altered and supplies of negotiable forms can be used for unauthorized purposes. Safeguarding of the Information System Assets is a very important function of each organisation.
The term IT infrastructure is a generic one used to describe the physical computer installations, the system software and the Information Systems process that support them.

The IS auditor will require to review the physical security over the facilities, the security over the systems software and the adequacy of the internal controls. The IT facilities must be protected against all hazards. The hazards can be accidental hazards or intentional hazards.

Accidental hazards include fire, flood, power failure etc. Fire starts accidentally or is the result of a deliberate attack. All the computer installations should take adequate precautions to ensure that fire can be prevented, detected and extinguished. Flooding can cause extensive damage to the computer systems. The power supply for the computer installation is a vital service need and the uninterrupted availability thereof has to be ensured to facilitate continuity in processing.

3.1.2 Maintenance of Data Integrity :

Data Integrity includes the safeguarding of the information against unauthorised addition, deletion, modification or alteration. This includes items such as accounting records, backup, documentation etc. Information Systems are used to capture, store, process, retrieve and transmit the data in a secure and efficient manner. The emphasis is on the accuracy of the data and its transmission in a secured manner. Data Integrity also implies that during the various phases of electronic processing, various features of the data viz. Accuracy, Confidentiality, Completeness, Up-to-date status, Reliability, Availability, Timeliness and Effectiveness are not compromised. In other words, data should remain accurate during electronic processing. The desired features of the data are described hereunder:

a) Accuracy : Data should be accurate. Inaccurate data may lead to wrong decisions and thereby, hindering the business development process.

b) Confidentiality: Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so. It also includes protecting the individual pieces of information that may seem harmless by the owner, but can be used to infer other confidential information.

c) Completeness: Data should be complete. Incomplete data loses its significance and importance.

d) Up-to-date Status : Data should be updated regularly. If the information is not up-to-date, it presents a false picture of the organization.

e) Reliability: Data should be reliable because all business decisions are taken on the basis of the current database.

f) Availability: Data should be available when an authorized user needs it. It should be ensured that the information services are unavailable to the unauthorised users.

g) Timeliness: Timeliness of the data is very important because if data is not available when required, the very purpose of maintaining the database gets defeated.

h) Effectiveness: Information should be effective, so that it helps in the process of business development and expansion.

If data integrity is not maintained, an organization loses its true representation. Poor data integrity could lead to loss of competitive advantage. Corruption of data would affect many users in a networked environment. If the data is valuable to a competitor, its loss may undermine an organization’s competitive position.

3.1.3 Maintenance of System Effectiveness :

An effective Information System significantly contributes to the achievement of the goals of an organization. Therefore, one of the objectives of IS audit is to verify system effectiveness. It provides input to decide when, what and how the system should be improved, so that its utility to the management is maximum.

The main objective of introducing computerization in the organisations in the banking and financial sector is to achieve the goals effectively and efficiently. The IS auditor's responsibility is to examine how the Information Systems assist in the achievement of each organisation's goals. System Effectiveness is a ratio of the actual output to the standard (budgeted) output. If it is more than 100%, effectiveness is achieved; or else, it shall be deemed that ineffectiveness has been introduced in the business process. Major goals and criteria of computerization are:

a) Improved Task Accomplishments: The Information Systems should improve the task accomplishment capacity of its users by enabling them to become more productive.
b) Improved Quality: It should improve overall quality of work and services by increased accuracy of information. It should also reduce the time required for retrieval of information.
c) Operational Effectiveness: The Information System should be operationally effective and easy to use. It should be frequently used and users must be satisfied with its performance.
d) Technical Effectiveness: The Information System should be equipped and upgraded by appropriate hardware and software from time to time.
e) Economic Effectiveness: The Information System should be fully utilized. Benefits derived should exceed the cost of procurement, implementation, operation and maintenance.

3.1.4 Ensuring System Efficiency :

The resources used by the Information Systems such as the machines, computer peripherals, software etc. are scarce and costly. Efficient Information Systems use minimum resources to achieve the desired objectives. When computer no longer has excess capacity, system efficiency becomes important. It becomes necessary to know whether the available capacity has been exhausted or the existing allocation of the computer resources are causing the bottlenecks.

The ratio of the output to the input is known as efficiency. If output is more with the same or less actual input, system efficiency is achieved; or else, the system is inefficient. If computerization results in the degradation of efficiency, the effort for making the process automated stands defeated. Hence, the assessment of the capabilities of the hardware and software against the workload of the environment is very essential. The IS auditors are responsible to examine how efficient the application software is in relation to the users and the workload of the environment. The system should assist in management planning and efficient execution thereof. The organisation should get maximum output using minimum resources. In this context, the efficient use of the hardware resources and their upgradation, as per requirements, is very essential. Automation should deliver the planned results with

less consumption of computer hardware, software, computerized operations and computer personnel.

3.1.5 Other Objectives :

The following could be, among others, considered the other objectives of IS audit :

a) Identify the risks that the organisation is exposed to in the existing computerized environment and to prioritize such risks for remedial action.

b) The implementation of Information Technology in the organisation is as per the parameters laid down in the Security Policy, as approved by the Board of Directors of the organisation.

c) Verify whether the Information System procedures and policies have been devised for the entire organisation and that the organisation's systems, procedures and practices are adhered to and that due prudence is exercised at all times in accordance with the circulars and instructions for a computerized environment, issued by the management of the organisation.

d) Verify whether proper security policies/procedures have been formulated and implemented regarding the duties of the system administrators, system maintainers and persons operating the system for daily operations.

e) Contribute effectively towards the minimization of computer abuses/ crimes by suggesting steps for removing any laxity observed in the physical and logical controls.

f) Suggest improvements in the security controls for the Information Systems.

g) Act as an advisor to the management of the organisation for improving security and IT implementation standards.

h) Adhere to the established norms of ethics and professional standards to ensure quality and consistency of audit work.

3.2 Scope of IS Audit:

The IS audit should cover all the computerized departments/offices of the organisation. The scope of IS audit should include the collection and evaluation of evidence/information to determine whether the Information Systems in use safeguard the assets, maintain data security, integrity and availability, achieve the organizational goals effectively and utilize the resources efficiently. The scope of IS audit should also include the processes for the planning and organization of the Information Systems activity, the processes for the monitoring of such activity and the examination of the adequacy of the organization and management of the IS specialist staff and the non-specialists with IS responsibilities to address the exposures of the organisation.

CHAPTER 4

Information Systems Audit Approaches

There are three approaches for conducting Information Systems Audit viz. auditing around the computer, auditing through the computer and auditing with the computer.

4.1 Auditing around the Computer:

Under this approach, the emphasis is on checking the correctness of the output data/documents with reference to the input of a process without going into the details of the processing involved. This approach is preferred, where auditors themselves do not have the

desired level of technical skills to adopt the other approaches. This is also preferred, when high reliance is placed on the users rather than the computer controls to safeguard the assets, maintain data integrity and attain effectiveness and efficiency objectives. The focus is on the procedural controls rather than the computer controls. This approach can be used in the following circumstances :

When an application system is simple, logic is straightforward and clear audit trail exists, this approach can be adopted. The process generates the audit trails such as the generation of exception reports along with the main reports. Such systems have very low inherent risk i.e. they are unlikely to be susceptible to material errors or irregularities or to be associated with significant ineffectiveness or inefficiencies in operations. Input transactions in such systems is in batch mode and control is maintained using traditional methods like the separation of duties and management supervision. Further, the task environment in such systems is relatively constant and the system itself is rarely modified.

This approach may be used when an application system uses a generalized package that is well tested and used by many users as its software platform. If the package has been provided by a reputed vendor, has received wide-spread use and appears error free, the auditors may decide to adopt this approach. Auditors should ensure that the organization has not modified the package and adequate controls exist over the source code and documentation to prevent unauthorized modification of the package.

When high reliance is placed on the users rather than the computer controls to safeguard the assets, maintain data integrity and attain effectiveness and efficiency objectives, this approach can be adopted.

Auditing around the computer is a simple approach. It does not provide any information about the system's ability to cope with the changes. Systems can be designed and programs can be written in certain ways to inhibit their degradation, when user requirements change. Further, this method cannot be used for complex systems. Otherwise, the auditors might fail to understand some aspects of a system that could have a significant effect on the audit approach.

4.2 Auditing through the Computer :

Auditing through the computer requires fair knowledge of the operating system, hardware being used and certain technical expertise in systems development. Under this approach, the computer programs and the data constitute the target of IS audit. Compliance and substantive tests are performed on the computer system, its software (both operating system and application system) and the data. IS auditors can test the application system effectively using this approach. The IS auditors can use computer to test logic and controls existing within the system and also records produced by the system. This approach increases the IS auditor's confidence in the reliability and applicability of the evidence/information collected and evaluated. This approach is time consuming, as it needs understanding of the internal working of an application system. It also needs some technical expertise.

4.3 Auditing with the Computer :

Under this approach, the computer system and its programs are used as tools in the audit process. The objective is to perform substantive tests using the computers and its programs. The data from the auditee's computer system are retrieved to an independent environment. Audit interrogation and query is carried out on such data, using special programs designed for the purpose. This method is used where :
a) Application system consists of a large volume of inputs, producing large volume of outputs and where the direct examination of the inputs/outputs is difficult.
b) Logic of the system is complex.
c) There are substantial gaps in the visible trails.

4.3.1 Computers are quite useful in the testing of transactions. Some of the software tools used for this purpose are briefly described hereunder :

4.3.1.1 Computer Assisted Audit Tools (CAATs) are efficient and effective ways to audit system-generated files, records and documents and to evaluate internal controls of an accounting system in many Information Systems. Computer Assisted Audit Tools are a practical means for conducting audit, wherever the information is available on the magnetic media alone. The technical papers relating to the use of the CAATs should be kept separate from the other audit working papers. The IS audit documentation should contain the description of the CAAT application.

4.3.1.2 Audit Software: It is a program, used by the auditors, to process data of audit significance from the auditee's accounting system. There are three types of such programs as under :

a) Package programs are designed to perform processing functions, creating data files and reports in a format specified by the auditor.
b) Special Purpose Programs are used to perform the audit tasks in specific circumstances and are prepared by the auditors or an outside programmer, engaged by the auditor.
c) Utility Programs are used to perform common data processing functions such as sorting, creating and printing files.

4.3.1.3 Test Data Techniques: A sample of data transactions is entered into the auditee's computer system and the results are compared with the predetermined results. CAATs are used to test the details of the sample transactions, the balances of the accounts, to identify unusual fluctuations, if any and general EDP controls like accessing the program libraries.

4.3.1.4 General Audit Software: It is the most widely used technique in conducting IS audit. Its use is limited by the skills of the personnel conducting the audit. Audit Command Language (ACL) is one such software. It is a tool for data analysis. It has the capabilities for Compliance and Substantive testing.

ACL is used to access, analyze, summarize or report data. Advantages of the ACL are as under:
a) It creates flexible reports and documents.
b) Auditors are independent of the technical experts for the data, access and process.

c) It increases audit coverage.
d) It saves time, money and effort. e) It helps gain control over and confidence in the audit results.
f) General Audit Software is not useful at application level.

Any Computer Assisted Audit Tool (CAAT) is as good as a data mining tool, which is used for extracting data from a data warehouse for MIS / Audit purposes. The following are a few of the generalized audit software in addition to ACL (ACL Services).
a) Audex 100 (Arthur & Andersons)
b) Pan Audit (Pansophic Systems)
c) Audit Aid (Seymour Schneidman & Co)
d) EDP Auditor (Cullinane Corporation)
e) Probe (Citibank)

CHAPTER 5
Information Systems Audit Methodology

5.1 Audit Methodology :

The IS audit work includes manual procedures, computer assisted procedures and fully automated procedures, depending on whether it is around, through, with or a combination of all these types of audit. In many cases, a combination of these techniques is required. The IS auditors may utilize the manual procedures when they are more effective than the other alternatives or when these procedures cannot be partially or fully automated. He/She should also use computer assisted procedures known as Computer Assisted Audit Tools (CAATs) because they permit the IS auditors to switch from the procedures based on limited, random and statistical samples of records in a file to a procedure that includes every record in a file.

5.2 Audit activity is broadly divided into 5 major steps for the convenience and effective conduct of audit.
a) Planning IS Audit
b) Tests of Controls
c) Tests of Transactions
d) Tests of Balances
e) Completion of Audit

a) Planning IS audit:

Planning is the first step of the IS audit. IS auditors should plan the audit work in a manner appropriate for meeting the audit objectives. As a part of the planning process, IS auditors should obtain an understanding of the auditee department/ office/organisation and its processes. It includes understanding of the objectives to be accomplished in the audit, collecting background information, assigning appropriate staff keeping in mind skills, aptitude etc. and identifying the areas of risk. Risk analysis of the operational system is carried out to identify the system with highest risks, considering the critical nature of the information processed through such system as well as the number and the value of the transactions processed. This is to identify the systems having the highest risk and to decide on the extent of the detailed analysis and testing to be conducted on those systems.

In this phase, IS auditors are required to understand the internal controls used within an organization. Various techniques can be used to understand the internal controls viz. review of previous audit reports/papers, interview/interaction with the management and Information Systems personnel, observation of activities carried out within the Information Systems function and review of Information Systems documentation.

b) Tests of Controls:

During this phase of IS audit, Internal Controls are tested to evaluate whether they operate effectively. This includes testing of management controls and application controls. The objective is to evaluate the reliability of the controls and find out weaknesses of the controls for meeting the IS audit objectives. IS auditor is required to make recommendations to rectify the weaknesses, observed during the course of an IS audit.
While carrying out tests of controls, the IS auditors should satisfy themselves regarding the following aspects of controls.

Identification: Organization should identify the controls to minimize the occurrence of unlawful events.
Implementation: Identified controls should be implemented.
Existence: Sometimes it happens that controls have been implemented, but in reality they do not exist due to various reasons. For example, the organization may have stipulated that the users should change their passwords every week. But, in reality this may not be happening. Physical existence of the controls is equally important.
Adequacy: IS auditors should examine the adequacy of the controls. They should see that the controls are adequate to cover all possible threats.
Documentation: All controls should be documented to make them effective.
Maintenance: Controls should be maintained intact on a continuous basis. For example, only the provision and installation of the fire extinguishers, smoke detectors, UPS etc. do not solve the problem. These instruments should be properly maintained, so that they serve the purpose, as and when needed.
Monitoring: Controls should be monitored by means of strict supervision, surprise checks, periodic inspection etc.

c) Tests of Transactions:

Tests of Transactions are used to evaluate whether erroneous transactions have led to a material misstatement of the financial information and whether the transactions have been handled effectively and efficiently. The objective is to evaluate data integrity. Some of such tests include the tracing of journal entries to their source documents, the examination of the price files, the testing of computational accuracy, the study of the transaction log etc. These tests are used to indicate the database system's effectiveness. CAATs are quite useful to perform these tests.

d) Tests of Balances:

During this phase of IS audit, final judgement is made on the extent of the losses or account misstatement that occur when Information Systems fail to safeguard assets, maintain data integrity and achieve system effectiveness and efficiency goals. As regards the safeguarding of assets and data integrity objectives, the typical substantive tests used are

confirmation of the receivables, physical verification of inventory and recalculation of depreciation on the fixed assets. Regarding the system effectiveness and system efficiency objectives, the tests to be conducted are in the process of evolution. For example, the shortcomings in the Information Systems Planning may have resulted in the purchase of inappropriate hardware. The system may provide outputs, but not of the required standards to make high quality decisions. During this phase of the IS audit, computer support is often required. General Audit Software can be used to select and print confirmations; expert systems can be used to estimate the likely bad debts and so on.

e) Completion of Audit:

This is the final stage of IS audit. Auditors are required to form their opinion, clearly indicating their findings, analysis and recommendations. Potential IS audit findings should be discussed with the appropriate/authorised personnel throughout the course of IS auditing. Preliminary conclusions and the audit findings should be presented to the auditee during an exit conference. All potential findings with sufficient merits and preliminary IS audit recommendations should be included for discussion in the exit conference. The exit meeting should document and include the auditee's comments and questions concerning the preliminary IS audit recommendations. The draft audit report should be the natural extension of the exit conference materials alongwith with the discussions that took place during the exit meeting. Once the auditee's responses have been received, the final audit report should be prepared and submitted to the designated authority/ management of the organisation.

Work papers used in the auditing should be well organized, clearly written and address all the areas included in IS audit. IS audit work papers should contain sufficient evidence/information of the tasks performed and the conclusions reached, including the results achieved, issues identified and authorized signatures approving the final opinion.
A typical audit report will include, among others, an introduction to the audit objectives, scope, general approach employed, summary of the critical findings, the data to support the critical findings, potential consequences of the weaknesses, auditee's responses and recommendations to rectify the weaknesses.

5.3 Sub-system Factoring :

IS audit is generally an exercise dealing with the complex Information Systems. In order to understand the complex system, it is always advisable to break the system into sub-systems. A sub-system is a component of a system that performs some basic functions needed by the overall system to attain its basic objectives. The process of breaking a system into sub-systems is called **factoring.** The process of factoring terminates when it is felt that the system has been broken into sub-systems, small enough to be understood and evaluated. Thus, a complicated system is divided into small sub-systems until it becomes easily understandable.

Once the system has been factored into several easily understandable subsystems, the task of the IS auditors is :
a) To evaluate the effectiveness of the controls in each sub-system.
b) To determine the implications of each sub-system's reliability visa-vis the overall

reliability/effectiveness of the system.

5.4 There are two main sets of systems, which require to be further factored into sub-systems for conducting IS audit.

5.4.1 Management Systems :
Management Systems provide stable and basic infrastructure facility on which the Information Systems can be built and operated on a day-to-day basis. Management Systems can be factored into sub-systems that perform Top-level Management, Information Systems Management, Systems Development Management, Programming Management, Data Administration, Quality Assurance Management, Security Administration and Operations Management.

Top-level Management is responsible for long-term policy decisions on the use of the Information Systems in the organisation.
Information Systems Management is responsible for planning and controlling the Information Systems activities in the organisation. It provides assistance to the top management for making long-term policies and translates the long-term policies into short-term goals and objectives.
Systems Development Management designs, implements and maintains the application systems.
Programming Management prepares programs for new systems, maintains old systems and provides general systems support software.
Data Administration addresses the planning and control issues in relation to the use of the database.
Quality Assurance Management ensures that the Information Systems development, implementation, operations and maintenance conform to the established quality standards.
Security Administration is responsible for access control and physical security over the Information Systems.
Operations Management plans and controls the day-to-day operations of the Information Systems.

5.4.2 Application Systems:
Application Systems undertake basic transactions processing, management reporting and decision support. They can be broken into sub-systems that perform boundary, input, communication, processing, database and output functions.

Boundary sub-system consists of the components that establish interface between the user and the system.
Input sub-system comprises the components that capture, prepare and enter commands and data into the system.
Communications sub-system consists of the components that transmit data among the sub-systems and systems.
Processing sub-system includes the components that perform decision making, computation, classification, ordering and summarization of the data in the system.
Database Sub-system comprises the components that define, add, access, modify and

delete data in the system.
Output Sub-system consists of the components that retrieve and present data to the users of the system.

5.5 Broad Framework for Conducting IS Audit :

A broad framework can be formed from the basic objectives of IS audit. In addition to this, IS audit evaluates the organizational set up and quality of administration. It should be noted that IS audit is not limited by laid down procedures. It is also important to keep one's eyes and ears open. The IS auditors should, therefore, analyze what they observe and hear. The main issue involved in IS audit is confidentiality of programs, files, access rights to files and focus on software application packages. The major concerns of the IS audit, as derived from its objectives, are as under:

A. Safeguarding Assets :

One of the prime objectives of any audit is to ensure that the assets of the organisation are safeguarded. In the computerized environment, the assets to be safeguarded are hardware, software, data and users. The yardstick to measure the importance of this objective is the expected loss that may be sustained by the organisation if the asset is destroyed, stolen, lying unutilized, service denied or used for unauthorized purposes. The IS auditors should verify that the assets are put to effective use in a secured environment. In order to determine whether the assets of the organisation are duly safeguarded, the IS auditors should inspect, among others, the following areas :

Environmental Security: It is very important for the effectiveness of all other protective measures stipulated or installed at the sites. The server room houses the all-important hardware. Its location should be a strategic one and not easily accessible. The server room should be exclusively for the server itself and the other items, equipment etc. should not be kept there.
Uninterrupted Power Supply : The uninterrupted power systems are meant for supplying conditioned and stabilized power to computer equipments at all times. It also provides stabilized power from battery storage when electricity fails. It is very important that the UPS functions properly when electricity fails. The UPS should be maintained regularly.
Electrical Lines: Electrical cabling and wiring constitute the basic components. Faulty electrical cabling and wiring are responsible for operational failures. There should be a separate and proper earthing for the dedicated electrical line.
Data Cabling: Information Technology experts estimate that 90 percent of the network problems are cable related. Hence, all possibilities of routing cables, locations of cable closets, sites of Switch, Router installation etc. should be explored before finalizing the plan. Detailed map of the cable lay out including Switches, Routers is very important to guide the hardware service engineer in the event of LAN cable fault. Further, electrical cable and data cable should not cross each other to avoid possible disturbance during data transfer.
Fire Protection: Fire alarm system, smoke detectors and fire extinguishers are very important to deal with the event of fire breaking out. Fire extinguishers are commonly filled with water, carbon dioxide or Halon. Little care is required while operating gas based extinguishers because they replace oxygen and thereby, extinguish the fire. Water is

effective. But, it is dangerous to use in proximity to live equipments. Dry powder or foam type extinguishers are not advisable because they leave deposits on the equipments.

Insurance: All critical computer equipments are required to be insured with reputed insurance firm/s to secure the Information System resources/assets of the organisation.

Annual Maintenance Contract: Periodic maintenance of the computers, network etc. is essential to ensure trouble free operations of the equipments. For this purpose, it is required that the annual maintenance contract is awarded and renewed in time. At the same time, it is also essential that the maintenance staff is available in time. There should be a proper record of the activities carried out during maintenance.

Logical Security: It restricts access to the system if the user fails to identify himself/herself to the system correctly . Login name/user ID and password are controls for this security. It is exercised at the operating system level and at the application system level. Logical security at the operating system level ensures the access to the computer system when it is successfully powered on, after its boot operation is completed. Logical security at the application system level gives access rights to specific application software depending on the responsibility and authority of the user. IS auditors should verify the effectiveness of the logical security in place by evaluating its controls. Secrecy and security of the user ID and password, different levels of access rights and their allocation to the users, creation of users, its records, users created for maintenance purpose and their termination on completion of the work, user log in status report, presence of dummy user ID in the system etc. are some of the points which require consideration of the IS auditors.

B. Data Integrity : Data is the most important resource in a computerized environment, which needs to be accurate, complete, consistent, up-to date and authentic. The IS auditors are concerned with the possibility of deviation from the standards. They are required to verify how well data integrity is maintained and find out any laxity therein.

The examination of the following points are very important in respect of data integrity:

Data Input Controls: The largest number of controls is available at the time of data entry in the system. Data Input Controls are error prone because the activities involved in data entry are of routine and monotonous nature. Data entry is also a major area for intentional fraudulent activity. It involves addition, deletion, modification or alteration of the input transactions or data. Hence, the IS auditors should minutely evaluate the effectiveness of the data input controls. The use of the scanner and inputs to the system through floppy should be monitored and controlled.

Data Processing Controls: The application system processes the data on-line on day-to-day basis. The IS auditors are concerned about the Data Processing Controls. They should examine that only designated/authorized officers perform start-of-day operation. The day end process should be completed with the generation of the prescribed reports. It is also required that proper record is maintained in respect of the corrections made in the database under authentication.

Patch Program: It uses the file structure of the existing database files and is capable of effecting changes in a data file. It bypasses the proper menu access controls provided by the application software system and does not leave any audit trail. It can add, modify, alter

and delete the data. The behavior of the approved programs are known and certified, but it is uncertain in the case of such patch programs. They usually bypass all the safeguards available to the system programs. They conveniently flout all norms to achieve results at any costs. Therefore, the IS auditors should verify that only approved programs are loaded in the system and the application programs are exactly identical with the list of the approved programs in respect of file name, file size, date and time of compilation. It is also necessary that a record be maintained regarding the patch programs used indicating the reasons under authentication.

Purging of Data Files : It is pruning of the data files of the identified past period for which it is no more necessary to store the data in the current system. Before undertaking the purging activity, it is necessary to take a backup of full data directory. The purging of the static data or master particulars is never taken. The IS auditors should examine that the purged data backup media is stacked in chronological order for easy tracing and also is in safe custody. A manual record of purging activity should also be maintained. The access to the purged data should be restricted and controlled to ensure the integrity of the purged data.

Data Backup : Data backup is an essential aspect of all computer operations. Some commonly used computer media include hard disk, floppy disks, tape cartridges, CD-ROMs, DVD ROMs etc. Off-site back-ups are taken on floppies or tape cartridges, while on-site back-up is taken on hard disks. Back-up is one of the measures of the business continuity planning and is also required for archiving of old records. It is necessary that the backups are taken regularly. One set of the backup requires to be stored off site. The backups have to be tested periodically by restoring the data therefrom. The backup media have to be verified periodically for readability. Backup media should be properly labeled and numbered. This is a very important area and requires proper attention.

Restoration of Data: It is defined as downloading of data afresh from magnetic media, in case of crash of the system, irrecoverable corruption or loss of data, for going back on line. Backup is taken at a particular point of time like beginning of day operations, end of day operations etc. Thus, restoration of data is dependent on the magnetic media and the data stored thereon. Restoration of the data is required in the event of major corruption of data. In the event of a virus attack or total destruction of a server or the computer site, the only option is to fall back upon the restoration option. Restoration of data helps to obtain a position of data as of a particular date, to establish whether any data tampering has taken place. It assists in conducting system audit as of a previous date and generates ledgers of previous years. Transactions of purged period can also be retrieved.

C. Business Continuity Planning: Disruption of operations can occur because of two types of problems. First, some minor problems like power failure, UPS failure, server failure, inability to read/restore backups, cable fault etc. can disrupt the operations. Second type of disruption can occur on account of natural calamities like fire, flood, building collapse or man made calamities like bomb blast, radiation, virus attack, induced data loss etc. Business Continuity Plan is prepared to recover from such kind of interruptions. It relates to a higher level of failure. It is all about anticipating any disastrous event and

planning adequately for the business to live through it. The IS auditors should verify the existence and operability of the Business Continuity Plan. They should also examine the awareness of the staff regarding the execution of the plan in a genuine emergency and comment upon its effectiveness. Business Continuity Plan should be documented and tested at regular intervals to assess its effectiveness.

BCP is required to satisfy short, medium and long-term recovery. In the short term, the essential systems and services are restored. Medium term plans are for recovering the organisation's systems and services on a temporary basis. Long term plans are for total recovery of the processing environment.

There are three methods of recovery namely cold, warm and hot backup sites. A cold site is where a computer room is provided in which equipment can be installed when needed. A warm site is a computer room filled with all the required equipment, but onto which all the software and applications must be loaded when it is needed. A hot site is one where the original installation is duplicated and ready to use when disaster occurs.

BCP should outline the responsibilities for all the recovery processes, procedures for reproducing the computer media, location of the backup media, priorities for recovery, sources of replacement hardware and software and alternative data communication facilities.

Output Reports: One of the basic principles in the computerized environment is known as GIGO i.e. "Garbage in Garbage out". This means that, if the input to the system is garbage (or meaningless), the output will also be garbage. Reports and printouts are generated in computerized environment to ensure the correctness of the inputs and processing. Reports are also important to ensure that the application system programs serve the needs of the organisation. Any lacunae or bugs in the application software can be located by checking the reports and printouts. The importance of checking the reports can never be over emphasized. The IS auditors should scrutinize output reports on sample basis to identify the trend, the quality of follow up and the control exercised by the management. The audit trail report should generate the user ID of the data entry operator and the authorized official for any addition, change, modification and deletion of transactions effected in the database. It should provide the evidence/information of unauthorized access outside the application menu. The IS auditors should verify whether the audit trail reports are generated and checked by the designated officials. Exceptional transaction report is also a very important report.

Version Control: Data integrity is very much dependent on the version of the software running in the system. Authorized Version of the software can lead to accurate processing. Non-standard programs are potential threat to integrity. A complete listing of the programs loaded in the system should be available on record for verification. The IS auditors should verify that licensed copies of the operating system and the application system software are used for computerized operations.

Virus Protection: Computer virus is a program that is self-replicating and can corrupt or

destroy data irretrievably. It resembles biological viruses in behavior. It may have a dormancy period and gets activated on a certain date. It is potentially disastrous. Anti-virus software is available and is capable of countering against known viruses, malicious programs. Anti-virus software is updated by the manufacturers on a regular basis to counter against the new viruses coming up. It is necessary to keep the anti-virus software updated at all times. All extraneous floppies and other media should be checked/scanned for virus before use.

D. System Effectiveness :

It is expected that the Information system should improve the overall quality of work including accuracy and time consumed in performing the tasks. Further, it should be user friendly. The IS auditors should judge how effective the system is in accomplishing the goals with which computerization was introduced.

E. System Efficiency :

The IS auditors should examine whether every computer asset is used to its maximum operational capacity.

F. Organization and Administration :

Efficiency in computerized operations is dependent on the efficiency of the personnel using the computer resources. Computer personnel should do their work completely, timely, accurately and that too, with minimum resources. They should deliver more output quantitatively and qualitatively. Proper placement of the computer personnel on the basis of their aptitude, skill, knowledge and experience is very important. Computer personnel should be used effectively and efficiently with proper security for the organisation to reap maximum advantages.

Segregation of duties, job description for each level, proper training to the staff, dual control aspect in performing important operations, designated system administrator with suitable back-up arrangement etc., are important points to be considered. Records of work assigned to the staff, rotation, training imparted, login name given etc. are to be checked/verified by the IS auditors.

CHAPTER 6
Audit Charter

The responsibility, authority and accountability of the information systems audit function, both internal and external, require to be appropriately documented in an audit charter or engagement letter, defining the responsibility, authority and accountability of the IS audit function. The IS auditor will require to determine how to achieve the implementation of the applicable IS audit standards, use professional judgement in their application and be prepared to justify any departure therefrom.

The IS auditor will require to have a clear mandate from the organization to perform the IS audit function. This mandate is ordinarily documented in an audit charter, which will require to be formally accepted by the IS auditor. The audit charter, for the audit function as a whole, will require to include the IS audit mandate.

6.1 Contents of the Audit Charter :

The audit charter should clearly address the three aspects of responsibility, authority and accountability of the IS auditor. Various aspects to be considered in this connection are as set out hereunder :

6.1.1 'Responsibility' should cover the following :

a) Mission Statement
b) Aims/goals
c) Scope
d) Objectives
e) Independence
f) Relationship with external audit
g) Auditee's requirements
h) Critical success factors
i) Key performance indicators
j) Other measures of performance

6.1.2 'Authority' should cover the following :

a) Risk Assessment
b) Right of access to information, personnel, locations and systems relevant to the performance of audit.
c) Scope or any limitations of scope
d) Functions to be audited
e) Auditee's expectations
f) Organisational structure, including reporting lines to the Board of Directors/Senior Management/ Designated Authority.
g) Gradation of IS audit officials/staff

6.1.3 Accountability should cover the following :

a) Reporting lines to senior management / Board of Directors / Designated Authority
b) Assignment performance appraisals
c) Personnel performance appraisals
d) Staffing/Career development
e) Auditees' rights
f) Independent quality reviews
g) Assessment of compliance with standards
h) Benchmarking performance and functions
i) Assessment of completion of the audit plan
j) Comparison of budget to actual costs
k) Agreed actions e.g. penalties when either party fails to carry out his responsibilities.

6.2 Communication with the Auditees :

6.2.1 Effective communication with the auditees involves consideration of the following :

a) Describing the service, its scope, its availability and timeliness of delivery.
b) Providing cost estimates or budgets, if they are available.

c) Describing problems and possible resolutions for them.
d) Providing adequate and readily accessible facilities for effective communication.
e) Determining the relationship between the service offered and the needs of the auditee.

6.2.2 The audit charter forms a sound basis for communication with the auditee and should include references to the service level agreements for such things as under :
a) Availability for unplanned work
b) Delivery of reports
c) Costs
d) Response to auditee's complaints
e) Quality of service
f) Review of performance
g) Communication with the auditee
h) Needs assessment
i) Control risk self-assessment
j) Agreement of terms of reference for audit
k) Reporting process
l) Agreement of findings

6.3 Quality Assurance Process :

The IS auditor should consider establishing a quality assurance process (e.g., interviews, customer satisfaction surveys, assignment performance surveys etc.) to understand the auditee's needs and expectations relevant to the IS audit function. These needs should be evaluated against the charter with a view to improving the service or changing the service delivery or audit charter, as necessary.

6.4 Engagement Letter :

6.4.1 Purpose :

Engagement letters are often used for individual assignments, setting out the scope and objectives of a relationship between the external IS audit agency and an organisation. The engagement letter should clearly address the three aspects of responsibility, authority and accountability. The following aspects should be considered while preparing the engagement letter for the IS auditor.

6.4.1.1 Under Responsibility, the following should be addressed :
a) Scope
b) Objectives
c) Independence
d) Risk assessment
e) Specific Auditee requirements
f) Deliverables

6.4.1.2 Under Authority, the following should be addressed :
a) Right of access to information, personnel, locations and systems relevant to the performance of the assignment.
b) Scope or any limitations of scope.
c) Documentary evidence/information of agreement to the terms and conditions of the

engagement.

6.4.1.3 Under Accountability, the following should be addressed :
a) Designated/Intended recipients of the reports
b) Auditees' rights
c) Quality reviews
d) Agreed completion dates
e) Agreed budgets/fees if available

CHAPTER 7
Planning Information Systems Audit

The IS auditor will require to plan the information systems audit work to address the audit objectives and to comply with the applicable professional auditing standards. The IS auditor should follow the guidelines, as under, for planning the information systems audit work. These guidelines cover the planning process, the identification of the levels of planning and the documentation of the work to be performed by the IS auditors. These guidelines also set out how the IS auditor should comply with the internationally accepted standards.

7.1 PLANNING : While planning the IS audit work, the IS auditor should consider the following factors :

7.1.1 Knowledge of the Organisation :

Before beginning IS auditing, the IS auditor's work should be planned in a manner appropriate for meeting the audit objectives. As a part of the planning process, the IS auditor should obtain an understanding of the organisation and its processes. In addition to giving the IS auditor an understanding of the organisation's operations and its IS requirements, this will assist the IS auditor in determining the levels of materiality of the IS resources being audited, as they relate to the objectives of the organisation. IS auditors should also establish the scope of the audit and perform a preliminary assessment of the internal controls over the functions being audited.

7.1.2 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 at which the audit is being performed. An organisation with unusual or complex operations may require the IS auditor to obtain a greater knowledge of the organisation than a similar organisation without specialised 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 than when the objectives are for limited functions. For example, an audit with the objective of evaluating controls over an organisation's payroll system would normally require a more thorough understanding of the organisation than an audit with the objective of testing controls over a specific program library system.

7.1.3 The IS auditor should gain an understanding of the types of events, transactions and practices that can have a significant effect on the functions being audited. Knowledge of the organisation should include the business and financial risks facing the organisation as

well as the conditions in the organisation's market place. The IS auditor should use this information in identifying potential problems, setting the scope of work, evaluating the audit evidence/information and considering the actions of the management for which the IS auditor should be alert.

7.2 Materiality :

7.2.1 In the planning process, the IS auditor should normally 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 programme for the audit work to be performed.

7.2.2. An assessment of the risks should be made to provide reasonable assurance that the material items will be adequately covered during the audit work. This assessment should identify the areas with relatively high risks of the existence of material problems.

7.3 Audit Programme :

7.3.1 A preliminary programme for an audit engagement should normally be established by the IS auditor before the start of work. This audit programme should be documented in a manner that will permit the IS auditor to record completion of portions of the audit and identify work that remains to be done. As the work progresses, the IS auditor should evaluate the adequacy of the audit programme, based on the evidence/information being gathered in the process of auditing and indicate the areas that might require extended examination.

7.3.2 In addition to a listing of the work to be done, the IS auditor should prepare a list of the resources required to complete the work, a schedule for the work and a budget.

7.3.3 During the course of the work, the IS auditor should consider changes to the audit programme based on the IS auditor's evaluation of the adequacy of the programme and the IS auditor's preliminary findings. The Management/ Designated Authority of the organisation will require to be communicated all such changes with justification therefor.

7.4 Internal Control Evaluation :

7.4.1 Most audit engagements should include an evaluation of internal controls either directly as a part of the audit objectives or as a basis for reliance upon information being gathered as a part of the audit. Where the objective is evaluation of internal controls, the IS auditor should distinguish between the types of engagements. When the objective is to assess the effectiveness of the controls over a period of time, the IS auditor should include the procedures appropriate for meeting the audit objectives and these procedures may include compliance testing of controls. When the objective is to identify the control procedures at a point in time, the audit plan could be less extensive.

7.4.2 When the IS auditor evaluates the internal controls for the purpose of placing reliance on the control procedures in support of the information/evidence/ information being gathered as part of the audit, the IS auditor should make a preliminary evaluation of the

internal controls and develop the audit plan on the basis of this evaluation. During an audit, the IS auditor should consider the appropriateness of this evaluation in determining the extent to which the internal controls can be relied upon during testing. For example, in using computer programs to test data files, the IS auditor should evaluate the controls over the program libraries containing programs, being used for audit purposes, to determine the extent to which these programs are protected from unauthorised destruction/modifications.

7.5 Documentation of the Audit Plan :

7.5.1 The IS auditor's plan should be documented in audit work papers to the extent necessary for the IS auditor to determine that the steps of the plan have been carried out.

7.5.2 The IS auditor's plan may be documented on paper or in other appropriate and retrievable form.

CHAPTER 8
Standards & Guidelines for IS Audit

8.1 The specialised nature of the Information Systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. Such standards will require to be internationally accepted standards only. This will ensure that the IS auditor performs auditing, conforming to the minimum level of acceptable performance and meeting the required professional responsibilities.

8.2 The IS auditing Standards define the mandatory requirements for IS auditing and reporting. The IS auditing Guidelines provide the guidance for the application of the IS auditing standards. The IS auditor should take care of how to achieve the implementation of the Standards, the use of professional judgement in the application of the Standards and should also be prepared to justify any departure/deviation therefrom in the IS auditing work.

8.3 The IS auditor shall prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.

8.4 IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems Security Professionals etc.

8.5 The profitability and the future viability of the organizations in the banking and financial sector increasingly depend on the continued, secured and uninterrupted operations of the Information Systems. Therefore, it is essential for the IS auditors to be conversant with various aspects of Information Technology and the developments taking place in this area. The role of the IS auditors is to see that the organization's assets are protected and suitable internal controls are in place to protect its information and information resources. IS audit is responsible for providing an organization with independent and objective views on the level of security that should be applied to the Information Systems. Computer Security on the other hand is responsible for implementing security in the computerized

environment. The IS auditor will learn to co-exist with the Computer Security function and work together for the benefit of the whole organization ensuring that professional standards are maintained at all times.

8.6 Major areas, which will require to be IS audited, are broadly as under:
a) Safeguarding of Assets
b) Data Integrity
c) System Effectiveness
d) System Efficiency
e) Organization and Administration
f) Business Continuity Operations

8.7 IS auditing of the above areas at the micro level are as under :

8.7.1 Safeguarding of Assets :

The IS auditors will require to concentrate on the following areas to ensure that the Information Systems Assets of the organisation are safeguarded:
a) Environmental Security
b) Data
c) Uninterrupted Power Supply
d) Electrical Lines
e) Data Cables & Networking Products
f) Fire Protection
g) Insurance of Assets
h) Annual Maintenance Contract
i) Logical Security & Access Control - Operating System Level
j) Logical Security & Access Control – Application System Level

8.7.1.1 The IS auditor shall be required to verify/inspect the following points in respect of the areas mentioned above.

A. Environmental Security :

The IS auditors should verify whether:
a) There is separate room for the server.
b) Server room has adequate space for operational requirements.
c) Server room is visible from a distance, but is not easily accessible.
d) Server room is away from the basement, water/drainage systems.
e) Server room can be locked and the key being under the custody of the authorized persons (System Administrator) only. Entry doors are protected by biometric/PIN or proximity key card access verification. Any failed attempts or system tampering as also unscheduled movement in restricted areas, glass breakage or the opening of doors will require to be logged and immediately reported to the Control Staff at the site. The biometric system will require to store all attempts at access.
f) To access any equipment in the Data Centre, one has to pass through (preferably) a minimum of two separate security doors, utilising biometric/PIN and/or proximity key card access verification facilities.
g) Server is not in close proximity to the UPS room.

h) Access to server room is restricted to authorized persons and activities in the server room are monitored.
i) Air-conditioning system provides adequate cooling.
j) Storage devices to keep stationary and other such items are not kept inside the server room.
k) All the walls with potential access will require to be heavily reinforced.
l) Humidity and heat measuring instruments like (Thermometer and Hygrometer) are installed in the server room.
m) Temperature readings are taken through out the raised floor and equipment areas, power rooms, basement, diesel fuel storage area, roof, generator, cooling towers, waiting and display areas.
n) Smoking, eating and drinking are prohibited in the server room to prevent spillage of food or liquid into sensitive computer equipment.
o) Briefcases, handbags and other packages are restricted from the server room, tape library and other sensitive computer area to prevent unauthorized removal of data held on removable media as also to prevent entry of unacceptable material into the area.
p) Server room is neat and clean to ensure dust free environment.
q) Scanners are kept in safe custody and access is restricted.
r) Floppy disk drives on the nodes can be disabled, if necessary for better security.
s) Steel bollards to be placed in the front of the building to prevent vehicular ingress.
t) Data Centre to be so choosen to have police protection and fire prevention services within a very short time, say, 5-10 minutes.

B. Uninterrupted Power Supply :

In addition to the availability of the Generator facility at the site, the IS auditor should verify whether:
a) There is a separate enclosure and locking arrangement for the UPS.
b) Maintenance agency provides battery service regularly.
c) There is a regular contract for maintenance of the UPS and the preventive maintenance is carried as per the contract.
d) The record of the tests undertaken is maintained to verify the satisfactory functioning of the UPS.
e) UPS cabin has adequate ventilation to take care of acid fumes emitted by the Lead Acid batteries.
f) Capacity of the UPS system is sufficient to take care of the electricity load required for computers installed.
g) UPS is free of the electricity load relating to the tube-lights, fans, water coolers etc.
h) UPS functions properly when electricity fails.

C. Electrical lines :

The IS auditors should verify whether:
a) There is a separate dedicated electrical line for the computer equipment.
b) Power supply to computer equipment is through UPS system only.
c) The electrical wiring looks concealed and is not hanging from ceiling or nodes.
d) The circuit breaker switches exist in locked condition only.

D. Data Cables :

The IS auditors should verify whether :

a) A map of the cable layout is kept in a secure place with proper authority. This is helpful in timely and fast repairs of LAN cable faults.

b) Cabling is properly identified and recorded as fiber optic, co-axial, unshielded twisted pair (UTP) or Shielded Twisted Pair (STP).

c) Electrical cable and data cable do not cross each other to avoid possible disturbance during data transfer within the network.

E. Fire Protection :

The IS auditors should verify whether:

a) Fire alarm system is installed.

b) Smoke detectors are provided in the server room and in the other areas of computer installations.

c) Smoke detectors are tested on a regular basis to ensure that they work.

d) Gas type (Carbon dioxide, Halon etc.) fire extinguishers are installed at strategic places like server room, UPS room and near the nodes and printers.

e) Dry powder or foam type extinguishers should not be used as they tend to leave deposits.

f) Staff knows how to use the fire extinguishers.

g) Fire extinguishers are regularly refilled/maintained.

h) An evacuation plan is documented and rehearsed at regular intervals for taking immediate action in the case of the outbreak of fire.

F. Insurance :

The IS auditors should verify whether:

a) All the computer equipments are covered under the appropriate electronic equipment insurance policy with a reputed insurance firm.

b) A record of the original policy is maintained with the detailed list of the equipments covered under the policy.

c) Information regarding shifting of computer equipment to or from or within the department/office is conveyed to the insurance firm.

d) Adequacy of the insurance cover should be verified as per the policy of the organisation.

G. Annual Maintenance Contract :

The IS auditors should verify whether:

a) Stamped agreements for maintenance contract are executed and available.

b) Activities carried out during maintenance have been reported in the registers and duly authenticated.

c) Contract renewal rates are maintained in the register.

d) Access for maintenance purpose is granted only on verifying the identity of the service person.

e) The maintenance staff support is available in time.

H. Logical Security & Access Control – Operating System Level :

The IS auditors should verify whether:

a) Access to the systems is only through password protected user IDs.

b) Operating System (OS) allots unique user identity (ID) for all users.
c) OS provides for different levels of access rights to volumes, directories and files.
d) OS prompts for change of the user password after the lapse of specified periods.
e) OS ensures secrecy and security of the user passwords and the access rights granted to a user.
f) Unrestricted access to the systems is provided only to the System Administrator.
g) Administration level access is restricted to authorized and limited persons.
h) All the security features available in the OS are enabled/taken advantage of as far as possible for ensuring better security.
i) Administration access should not be available to the officials who are under notice period, retiring shortly, under disciplinary action etc.
j) OS provides for loading of virus prevention software and is implemented.
k) Record is maintained and authenticated regarding the installation of the Operating System, its up-gradation, re-installation and maintenance.
l) A register is maintained in respect of all the OS level users, giving the details such as the date of creation, suspension, cancellation, access rights granted, purpose of creation etc.
m) Users created for audit/maintenance purpose are disabled immediately after the work is over.
n) The department reviews the number of the OS level users periodically.

I. Logical Security & Access Control – Application System Level :

The IS auditors should verify whether:
a) System provides for unique user IDs and password for all users.
b) System provides for different levels of access.
c) System prompts for change of user password after lapse of specified period.
d) System ensures secrecy and security of the user passwords and the access rights granted to users.
e) Unrestricted access to the entire application system menus is provided only to a Super User.
f) Application makes use of all the security features available at the Application System level.
g) Super User access in application level is not given to staff who is under notice period, retiring shortly, under disciplinary action etc.
h) The application system user list is periodically reviewed.
i) The access privileges granted in the system are in accordance with the designation/duties performed.
j) None of the staff members has multiple level or duplicate access ID in the system.
k) Allocation of the suspended, disabled user ID to new users is avoided.
l) Active user IDs of the transferred, retired, suspended or dismissed employees are not present in the system.
m) There is no dummy user ID created in the system.
n) The user ID of staff on long leave, training etc. is suspended.
o) System logs out automatically if the user is inactive for a specified time (or user co sciously logs out when he/she leaves a terminal).
p) System does not allow concurrent login to a single user ID from different nodes.
q) Users, created for maintenance purpose, are cancelled on completion of the job.

r) The system does not allow user to cancel his/her own user ID. s) Authority periodically reviews the user login status report.
t) Users do not share their passwords.
u) Passwords of alphanumeric characters are used.
v) Users do not write their passwords on wall, desk diary etc. and are aware of the need for the secrecy of their passwords.
w) System automatically locks the user ID after unsuccessful login attempts.
x) User log indicating date, time, node, user ID, transactions performed etc. are generated by the system and evaluated by the System Administrator.

8.7.2 Data Integrity :

The IS auditor will require to address, among others, the following areas under IS auditing :
a) Data Input Controls
b) Data Processing Controls
c) Patch Programs
d) Purging of Data Files
e) Backup of data
f) Restoration of Data
g) Business Continuity Planning
h) Output Reports
i) Version Control
j) Virus Protection

A. Data Input Controls :

The organisations in the banking and financial sector undertake diverse activities relating to the receipt of deposits, advancement of credit, investment of funds etc.Further, the areas of operation and the level of economic activities could also be different. All these activities, the transactions resulting therefrom, the data inputs required therefor including the data input controls to be in place in the organisation will require to be judiciously addressed. However, illustratively, such data input controls may relate to the following areas of activity and the IS auditors will require to verify the same.

a) History of signatures scanned is available in the system.
b) The entire stock of cheque books is fed to the system.
c) The cheque books issued are entered and confirmed in the system on day-to-day basis.
d) The data fed in to various accounts including the customer accounts is accurate and correct.
e) Clear administrative guidelines exist regarding the access to live data.
f) Clear guidelines exist for on-line transactions including those put through the INTERNET by the Customers.
g) Data Administration is a part of System Administration. However, Database Administration is separate from System Administration.
h) Data Owner(DA) and Database Administrator (DBA) are independent of both the systems development and operational activities.
i) The roles of DA and DBA are clearly defined in respect of , among others, (i) definition, creation & retirement of data, (ii) database availability to Users, (iii) information and services to Users, (iv) maintenance of database integrity and (v) monitoring and

performance.

B. Data Processing Controls :

The IS auditor should verify whether:

a) The designated/authorized officials do start-of-day process.

b) The operating staff pay attention to the error messages displayed on the screen and initiates corrective action.

c) Entries are cancelled only by the appropriate authority.

d) Cash entries are not deleted from the system. e) Prescribed reports are generated at the end-of-day process.

f) Printouts are scrutinized and preserved.

g) Proper record is maintained in respect of the corrections made in database under authentication.

h) Master data printouts are preserved carefully

i) Input to the system through floppy is monitored and controlled. j) Use of the scanner is monitored and controlled.

C. Patch Programs :

The IS auditors should verify whether:

a) The application programs are exactly identical with the standard list of approved programs in respect of file name, file size, date and time of compilation.

b) Only approved programs have been loaded in the system.

c) There are programs other than the approved ones.

d) There is a record of the patch programs used and the reason thereof under authentication.

D. Purging of Data Files :

The IS auditors should verify whether:

a) Purging activity is recorded and maintained in a register.

b) Purged backup media is kept properly under safe custody.

c) Access to purged data is restricted.

E. Back up of Data :

The IS auditors should verify whether:

a) All the floppies/CDs/tapes, purchased, pertaining to the OS software, application software and utility programs, drivers etc. are recorded in a register and properly stored.

b) Hardware, software, operating system, printer manuals are properly labelled and maintained.

c) Latest user manuals of the application software and other end-user packages running on the system are available for guidance.

d) Daily/weekly/monthly and quarterly back-up of data is taken without fail and is available (as per requirement).

e) Backup tapes are properly labeled and numbered.

f) Proper storage procedures and facilities are in place for backup copies.

g) There is offsite storage of one set of the backup data.

h) Backup tapes are verified/tested periodically by restoring the data and record

maintained.

i) Back up media is verified periodically for readability.

j) Record is available in respect of such verification.

k) Backup media are phased out of use after a specified period.

l) Backup register is maintained wherein all the events pertaining to the backup including the procedure of backup are recorded.

m) Physical and fire protection is provided to backup media.

F. Restoration of Data :

The IS auditors should verify whether:

a) The instructions for restoration of the back-up data have been compiled.

b) The data integrity is verified after the restoration work is over.

c) Activities carried out during the restoration work are recorded indicating date, time, reason for restoration and size of the data restored.

G. Business Continuity Planning (BCP) :

The IS auditors should verify whether:

a) Business continuity plan has been documented.

b) BCP covers all levels of disaster from partial to total destruction of facilities and contains guidelines to help determine the level of recovery necessary.

c) A copy of the plan is securely stored off site.

d) Detailed restart procedure has been documented in the plan.

e) BCP has been tested and is regularly tested to assess its effectiveness.

f) There is awareness among the staff members about the BCP and the modalities of its execution in case of an emergency.

g) Ready or alternate source of hardware/software is there to resume business activity within the shortest possible time after disruption.

h) A reliable backup of data and software is available all the times for restoration.

H. Output Reports :

The IS auditors should verify whether:

a) The audit trail report generates the user ID of the operator and the official for any addition / modification / deletion of the transaction data effected in the database.

b) Audit trail report is generated daily. Entries are scrutinized and verified.

c) Audit trail report indicates the evidence/information of unauthorized access outside application menu.

d) List of the cancelled entries is scrutinized and reasons for cancellation are recorded.

G. Version Control :

The IS auditors should verify whether:

a) The computer system has authorized version of an OS, authorized version of anti-virus software with its latest updates.

b) There exist the documentary evidence/information about the authenticity and the right to use the copy of the OS software, OS system utility, third party software, the runtime system of specified language or database in use and the anti-virus software.

c) Legally licensed copies of the software are used for computerized operations and the

licenses are currently in force.
d) Changes made to the application software with the approval from the controlling office/ department.

H. Virus Protection :
The IS auditors should verify whether:
a) Anti virus software is loaded in the system.
b) Anti virus software is regularly updated to cover software updates against the latest viruses.
c) All extraneous floppies are checked for virus including the floppies carried by the IS auditors.

8.7.3 System Effectiveness :
The IS auditors should verify whether:
a) Computerized operations provide better customer service in terms of time and quality.
b) Staff serves a larger number of customers during the day than prior to the introduction of online operations.
c) Customer information is provided timely and accurately.
d) The system reflects any improvement in the overall quality of products and services offered.
e) System has improved the tasks accomplishment capacity of its users by enabling them to be more productive.
f) Users are satisfied with the performance of the system.
g) System is user friendly and takes less effort.
h) The users are putting the software to frequent use, which requires less effort and is easier to use and the users are satisfied with the performance of the software.

8.7.4 System Efficiency :
The IS auditors should verify whether :
a) Department/Office ensures the use of every computer asset.
b) Department/Office utilizes every computer asset to its optimum capacity.
c) Periodical maintenance of the hardware asset ensures its uninterrupted service.
d) The online operations help complete day's workload on the same day consuming less time than the time taken for the respective manual operations.
e) The online operations provide accurate, complete and consistent data at each stage of processing.
f) Department/Office takes consistency check of balances daily to aid in the detection of errors or fraud.
g) Department/Office uses the hardware peripherals such as printers, nodes etc. efficiently.

8.7.5 Organisation and Administration :
The IS auditors should verify whether:
a) There is an Information Systems Security Programme for the entire organisation, approved by the Board of Directors.
b) There is a Corporate Information Systems Security Policy, well defined and

documented and implemented including Information Systems Awareness Programme.

c) There is an established hierarchy in the organisation with a Senior Executive in charge of the implementation of the Corporate Security Policy with Information Systems Security Officials at various levels in an Office.

d) Identified System Administrator for each computerised Office / Department, as required.

e) Job description for each level is prepared and implemented (including System Administrator).

f) Training is imparted to all staff members in turn for better results and output.

g) The entire staff is involved/motivated for working in the online environment.

h) The department allots online jobs to staff members accessing performance parameters like willingness, aptitude, expertise, skill, experience and knowledge.

i) Record is maintained showing details of the work assigned, period of assignment, rotation, training imparted, login name and acknowledgement obtained.

j) Dual control aspect is implemented for the important online operations.

k) The functions of initiating, authorizing, inputting, processing and checking of the data are separated to ensure that no person has complete control over a particular function. Therefore, abuse of that function is not possible without collusion between two or more individuals.

l) Rotation of duties is carried out at regular intervals.

m) System Administrator is supervised and controlled with respect to the creation of user ids at the OS level and Application Software level.

n) There are at least 2 persons for key functions of online operations to take care of absenteeism.

o) Department/Office ensures to bring up the servers into operation readiness sufficiently in advance before the commencement of the business hours.

p) Computers are covered to keep them free from dust, rain water etc.

q) Clear communication from the Management of the organisation to the effect that each member of the staff is responsible for maintaining security in the organisation, as per the Security Policy.

CHAPTER 9
Audit Sampling

9.1 During the course of the audit, the Information Systems Auditor is to obtain sufficient, reliable, relevant and useful information/evidence/information to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this information/ evidence/information. The IS auditor has to design and select an audit sample and evaluate the sample results. Appropriate sampling and evaluation will meet the requirements of “sufficient, reliable, relevant and useful evidence/information” and “supported by appropriate analysis”. The IS auditor should select the techniques, which result in a representative sample statistically for performing the compliance or substantive testing. Examples of compliance testing of the internal controls, where sampling could be considered, should, among others, include user access rights, program change control procedures, documentation procedures, program documentation, follow up of exceptions, review of logs, software license audits etc. Examples of the substantive tests, where sampling could be considered, should, among

others, include re-performance of a complex calculation (e.g. calculation of interest) on a sample of accounts, sample of transactions, supporting documentation etc.

9.2 Audit Sampling :

9.2.1 When using either statistical or non-statistical sampling methods, the IS auditor should design and select an audit sample, perform audit procedures and evaluate sample results to obtain sufficient, reliable, relevant and useful audit evidence/information.

9.2.2 In forming an audit opinion, the IS auditor should not examine all of the information available, as it may be impractical and valid conclusions could be reached using audit sampling.

9.2.3 Audit sampling is defined as the application of the audit procedures to less than 100% of the population to enable the IS auditor to evaluate the audit evidence/information about some characteristics of the items selected in order to form or assist in forming a conclusion concerning the population.

9.2.4 Statistical sampling involves the use of techniques from which mathematically constructed conclusions regarding the population can be drawn.

9.2.5 Non-statistical sampling is not statistically based and the results should not be extrapolated over the population, as the sample is unlikely to be representative of the population.

9.3 Design of the Sample :

9.3.1 When designing the size and structure of an audit sample, the IS auditors should consider the specific audit objectives, the nature of the population and the sampling and selection methods.

9.3.2 The IS auditor should consider the need to involve appropriate specialists in the design and analysis of the samples.

9.3.3 Sampling Unit - The sampling unit will depend on the purpose of the sample. For compliance testing of the internal controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g. a control such as an authorisation on an invoice). For substantive testing, variable or estimation sampling is frequently used, where the sampling unit is often monetary.

9.3.4 Audit Objectives - The IS auditor should consider the specific audit objectives to be achieved and the audit procedures, which are most likely to achieve those objectives. In addition, when audit sampling is appropriate, consideration should be given to the nature of the audit evidence/information sought and possible error conditions.

9.3.5 Population - The population is the entire set of data from which the IS auditor wishes to sample in order to reach a conclusion on the population. Therefore, the population from which the sample is drawn has to be appropriate and verified as complete for the specific audit objective.

9.3.6 Stratification - To assist in the efficient and effective design of the sample, stratification may be appropriate. Stratification is the process of dividing a population into sub-populations with similar characteristics, explicitly defined, so that each sampling unit can belong to only one stratum.

9.3.7 Sample Size - When determining the sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which the errors are expected.

9.3.8 Sampling Risk - Sampling risk arises from the possibility that the IS auditor's conclusion may be different from the conclusion that would be reached, if the entire population were subjected to the same audit procedure. There are two types of sampling risk.

9.3.8.1 Risk of Incorrect Acceptance - The risk that material misstatement is assessed as unlikely, when in fact the population is materially misstated.

9.3.8.2 Risk of Incorrect Rejection - The risk that material misstatement is assessed as likely, when in fact the population is not materially misstated.

9.3.9 Sample size is affected by the level of sampling risk that the IS auditor is willing to accept. Sampling risk should also be considered in relation to the audit risk model and its components, inherent risk, control risk and detection risk.

9.3.10 Tolerable Error - Tolerable error is the maximum error in the population that the IS auditor is willing to accept and still conclude that the audit objective has been achieved. For substantive tests, tolerable error is related to the IS auditor's judgement about materiality. In compliance tests, it is the maximum rate of deviation from the prescribed control procedure that the IS auditor is willing to accept.

9.3.11 Expected Error - If the IS auditor expects errors to be present in the population, a larger sample than the sample, when no error is expected ordinarily, has to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the IS auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures and evidence/information available from an evaluation of the system of internal controls and results from analytical review procedures.

9.4 Selection of the Sample :

There are four commonly used sampling methods:

9.4.1 Statistical Sampling Methods :

9.4.1.1 Random Sampling – It ensures that all combinations of sampling units in the population have an equal chance of selection.

9.4.1.2 Systematic Sampling – It involves the selection of sampling units, using a fixed interval between the selections, the first interval having a random start. Examples include Monetary Unit Sampling or Value Weighted selection, where each individual monetary value (e.g. INR1/$1) in the population is given an equal chance of selection. As the individual monetary unit cannot ordinarily be examined separately, the item which includes that monetary unit is selected for examination. This method systematically weighs the selection in favour of the larger amounts, but still gives every monetary value an equal opportunity for selection. Another example includes selecting every 'nth' sampling unit

9.4.2 Non-Statistical Sampling Methods :

9.4.2.1 Haphazard Sampling - The IS auditor selects the sample without following a structured technique, avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population.

9.4.2.2 Judgemental Sampling - The IS auditor places a bias on the sample (e.g. all sampling units over a certain value, all for a specific type of exception, all negatives, all new users etc.). It should be noted that a judgemental sample is not statistically based and results should not be extrapolated over the population, as the sample is unlikely to be

representative of the population.

9.4.3 The IS auditor should select sample items in such a way that the sample is expected to be representative of the population regarding the characteristics being tested i.e. using statistical sampling methods. In order to maintain audit independence, the IS auditor should ensure that the population is complete and control the selection of the sample.

9.4.4 For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected i.e. statistical sampling methods.

9.4.5 There are two commonly used selection methods such as Selection on Records and Selection on Quantitative Fields (e.g. monetary units).

For Selection on Records, the common methods are:

- Random Sample (statistical sample)
- Haphazard Sample (non-statistical sample)
- Judgemental Sample (non-statistical sample with high probability to lead to a biased conclusion)

For Selection on Quantitative Fields, the common methods are:

- Random Sample (statistical sample on monetary units)
- Fixed Interval Sample (Statistical sample using a fixed interval)
- Cell Sample (statistical sample using random selection in an interval)

9.5 Documentation :

The audit work papers should include sufficient details to describe clearly the sampling objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g. random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and the conclusions reached.

9.6 Evaluation of Sample Results :

9.6.1 Having performed, on each sample item, those audit procedures which are appropriate to the particular audit objective, the IS auditor should analyse any possible errors detected in the sample to determine whether they are actually errors and if appropriate, the nature and cause of such errors. For those that are assessed as errors, the errors should be projected as appropriate to the population, if the sampling method used, is statistically based.

9.6.2 Any possible errors detected in the sample should be reviewed to determine whether they are actually errors. The IS auditor should consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effects of the error on the other phases of the IS audit. Errors that are the result of the breakdown of an automated process ordinarily have wider implications for error rates than human error.

9.6.3 When the expected audit evidence/information regarding a specific sample item cannot be obtained, the IS auditor may be able to obtain sufficient appropriate audit evidence/information through performing alternative procedures on the item selected.

9.6.4 The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating the probable error in the population

and estimating any further error that might not have been detected because of the lack of precision of the technique together with the qualitative aspects of any errors found.

9.6.5 The IS auditor should consider whether errors in the population might exceed the tolerable error by comparing the projected population error to the tolerable error, taking into account the results of the other audit procedures, relevant to the audit objective. When the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk and if that risk is unacceptable, should consider extending the audit procedures or should consider performing alternative audit procedures.

CHAPTER 10

Information Technology, Security Issues and Information Systems Audit

10.1 Information Technology offers an easy and efficient way to collect, store, process and transmit information to any organisation and the organisations in the banking and financial sector are no exception. Vital business decisions are made by the organisations on the basis of this information and therefore, it is imperative to ensure that right information is available at the right time to the right people. Further, adequate security controls have also to be in place in an organisation to ensure that the information and the information systems remain inaccessible to unauthorized persons. Information stored in the computer systems and transmitted through networks will require to be protected. The protection of information becomes critical, when it is fund-based or represents sensitive/ confidential data like personnel records.

10.2 Information Technology will continue to advance, providing better and more powerful tools to the organizations, to acquire, store, process and network data. Today, network is an integral part of the day-to-day business operations in almost all organisations in the banking and financial sector. This has facilitated the sharing of information and the information systems in and between organisations, where required. However, the networking environment has also added to the immediate need for robust and rugged security controls relating to computer hardware, software, application software, communication systems and data.

10.3 The need for security controls assumes greater importance in view of the advent of Internet, the global internetworking phenomenon. Connecting to the Internet without strong security architecture in place can have severe consequences for an organisation. The extent of criminal activities in the Internet based environment is expected to grow alongwith advancement in Information Technology. Each organisation on the Internet has to unavoidably address, among others, the following security issues :

a) Unauthorized access to Information & Information Systems.
b) Loss/Modifications/Manipulations of data.
c) Loss of confidential information.
d) Problems inherent in an open Network (eg. viruses, Worms, sabotage, hacking etc.).

10.4 The survival of the banks and the financial institutions depends on the security infrastructure built up by each organisation for ensuring the accessibility, quality, adequacy and integrity of its information and Information Systems. The security measures for safeguarding the information resources will require to include the identification and

assessment of risks and the development of proper controls to offset/reduce possible threats.

10.5 Information Systems Audit (IS audit) :

Setting up of a secure Information System goes beyond mere computerization of manual process. The system should safeguard its assets and maintain data integrity. It should help in achieving the organization's goals. A secure information system is expected to have established comprehensive procedures and controls, which are backed by commitment from the management. It is required to periodically monitor that these procedures and controls are in place and operational to effectively ensure that the information stored in these systems continues to be dependable. Periodical monitoring is achieved by IS audit. IS audit is a process of collecting and evaluating evidence/information to determine whether a computer system could :

a) safeguard its assets (hardware, software and data) through adoption of adequate security control measures ;
b) maintain data integrity ;
c) achieve goals of the organization effectively ; and
d) result in the efficient use of the available Information System resources.

10.6 Data integrity means that the attributes like completeness, accuracy, timeliness, effectiveness and reliability of the data are consistently maintained during input processing, communication, storage and retrieval.

10.7 IS audit is an independent subset of normal audit process. The overall objective and scope of an audit do not change in the computerized environment.

In other words, it is an independent appraisal activity, which identifies security and processing risks in the computerized Information Systems and evaluates related manual and system controls to ensure security and reliability of hardware, operating system, system software, application software, communication systems as also to ensure integrity, confidentiality, authentication, non-repudiation and availability of data.

10.8 IS audit assumes greater importance in the context of the accelerated pace of computerization taking place in the banking and financial sector in the country. Uncontrolled use of computers can cause loss of important data. Inaccurate or untimely data can lead to incorrect decision making. Computer frauds, caused by outsiders or insiders, can land the banking and financial organisations in serious trouble. The absence of adequate security controls and necessary perpetual vigilant mechanism would render the detection of computer frauds a matter of chance only. Computer error can prove costly in the long run and loss of confidential data or loss of confidentiality of data can lead to loss of reputation and legal wrangles.

10.9 The following factors have contributed to the inevitability of IS audit:

a) An organization's ability to survive can get severely undermined through corruption or destruction of its information and information systems.

b) There is a possibility of misallocation of resources because of decisions based on incorrect data or poor quality Information Systems.

c) If computer system is not controlled, the possibilities of misuse can be very high.

d) Computer hardware, software and personnel are valuable assets of any organisation and hence, require to be utilised optimally.

e) Computer errors may result in huge financial loss.

10.10 Security Controls :

IS auditors are required to evaluate the effectiveness of the security controls. It is, therefore, important for the IS auditors to understand the nature of the security controls in place. A control is defined as a system which prevents, detects or corrects unlawful events. An unlawful event is an event, which arises if unauthorized, inaccurate, incomplete, ineffective or inefficient input enters in to the system. Control as a system consists of the policies, procedures, practices and organizational structures, designed to provide reasonable assurance that the business objectives of the organisation will be achieved and that the undesired events will be prevented or detected and corrected.

10.11 Organisations & Exposures :

Each organization will require to identify the events and circumstances, whose occurrence could result in a loss to the organization. These are called exposures. Controls are those acts/measures, which the organization must implement to minimize these exposures. Controls are broadly of the following types :

a) Deterrent Controls : Deterrent Controls are designed to deter unauthorised people, internal as well as external, from accessing the information and information systems.

b) Preventive Controls : Preventive Controls prevent the cause of exposure from occurring or at least minimize the probability of the occurrence of unlawful events.

c) Detective Controls : When a cause of exposure has occurred, detective controls report its existence in an effort to arrest further damage or minimize the extent of damage. Detective controls limit the losses, if an unlawful event at all occurs.

d) Corrective Controls : Corrective Controls are designed to help the organization recover from a loss situation. Business Continuity Planning is a corrective control. Without corrective controls in place, the organisation will suffer from the risk of loss of business and other losses, due to its inability to recover essential IT based services, information and other resources after the disaster has taken place.

IS auditors will require to ascertain that adequate control exists to cover each likely unlawful event. If the unlawful event is covered by a control, the IS auditors will require to evaluate whether the control is operating effectively. If more than one control covers an unlawful event (i.e. redundant controls), the IS auditors will require to verify that all these controls operate effectively.

10.12 Information Systems Audit & Benefits :

The IS audit assesses the strengths and weaknesses of the Information Systems. It also assesses whether each Information System actually translates itself into an effective tool to meet the business goals of the organisation. The following major benefits are expected from the conduct of IS audit :

a) IS audit can be equated to a preventive tool. It would identify the risks that an organisation is exposed to in a computerized environment. On identification of the risks, remedial measures can be taken to protect the interests of the organisation.

b) Regular conduct of IS audit would deter people/employees/users from indulging in manipulation of data, frauds etc. Any laxity in the controls/security of the Information Systems could be eliminated if IS audit is conducted at regular intervals. Regular conduct of IS audit and proper follow-up on the suggestions/recommendations in the IS audit report will provide the management reasonable assurance about the functionality and the security related performance capability of the Information Systems.

c) Security features and controls in a computerized Information System could be assessed and further improved, based on the suggestions/recommendations made in the IS audit report.

d) IS audit can verify whether there exists appropriate security infrastructure in the organization for safeguarding the information and the Information Systems.

e) IS audit assesses the health of the Information Systems in an organisation.

Conclusions and recommendations emerging from an IS audit shall influence the decision making process of the management regarding the security infrastructure in the organisation.

CHAPTER 11

IS Auditing and Skills

11.1 The knowledge required to audit information systems is extensive. For example, IS auditing involves as under :

a) Application of risk-oriented audit approaches.

b) Use of computer assisted audit tools and techniques.

c) Application of internationally accepted standards to improve and implement quality systems in software development.

d) Understanding of the organisational expectations in the auditing of the application systems under development as also the packaged software and project management.

e) Evaluation of the Systems Development Life Cycle (SDLC) or new development techniques (e.g. prototyping, end-user computing, rapid systems or application development).

11.2 The IS audit differs from the traditional audit in the sense that it requires adequate knowledge of computer systems in addition to the basic concepts of normal auditing. Information Technology is rapidly changing. It is essential that the IS auditors keep themselves abreast of the latest systems and techniques of IS auditing. The IS auditors will require to be well prepared, as under, to perform IS auditing :

a) A general understanding of the operating systems in use.

b) Thorough knowledge of the application software in use.

c) Knowledge of the automated operations, methods of storing and retrieval of data and controls used in the systems.

d) Knowledge of the methodology used in data processing.

e) IS auditors for auditing complex systems require substantial knowledge about the development, implementation and operation of the systems. A thorough understanding of various controls in the development of systems, maintenance of data and network management is essential.

f) An understanding of the emerging technologies, capacity to determine their impact on controls, ability to change audit procedures suitably and to develop evidence/information collection tools and techniques.

g) IS auditors should maintain technical proficiency. They should keep themselves informed about the current changes in the procedures, technologies adopted and the functions computerized by the organisations in the banking and financial sector.

h) Ability to identify general security measures including risk analysis.

i) Capabilities to render constructive disaster assessment.

j) Sound knowledge of the organisation’s accounting practice and the record keeping

requirements.

k) Ability to investigate thoroughly and to document the investigation work.

l) The audit process requires initiative, thoroughness and tact while addressing an audit assignment.

m) IS audit calls for understanding and the capabilities to analyze and offer constructive comments on the Information Systems Security and Controls.

n) All material irregularities are required to be reported and the IS auditor should report all the unpleasant findings.

o) The IS auditors should be aware of the situations where too much trust has been placed on one individual. One person acting alone could commit an error willfully or defraud the organisation. This is important in those transactions, which are perceived to be of high risk.

p) Capacity to plan and supervise IS audit to assure that the audit meets the desired objectives, as set out in the audit assignment, efficiently.

q) Knowledge of the basics in computer programming would help in having clarity of approach.

11.3 The IS auditors should meet at least the following eight technical proficiency requirements :

a) Proficiency as an auditor.

b) Ability to review and evaluate IS internal controls.

c) Understanding of the Information System's design and operations.

d) Knowledge of programming languages and techniques and the ability to apply computer assisted audit tools and to assess their results.

e) Knowledge of computer operating systems and software.

f) Ability to identify and reconcile problems with the client data file format and structure.

g) Ability to bridge the communication gap between the auditor and the IS professional, providing support and advice to the management of the organisation.

h) Knowledge of when to seek the assistance of an IS Professional.

11.4 It is not enough if the IS auditors have technical skills only to successfully diagnose the security control issues or the associated problems. They must also be able to clearly communicate key issues to the senior executives/ management/designated authority of the organisation, both orally and in writing.

CHAPTER 12

Audit Considerations for Irregularities

12.1 Due professional care and the observance of the internationally accepted professional auditing standards have to be exercised by the IS auditor in all aspects of IS auditing. The Information Systems Auditor will require to plan the information systems audit work to address the audit objectives and to comply with internationally accepted professional auditing standards. Further, during the course of IS auditing, the Information Systems Auditor will require to obtain sufficient, reliable, relevant and useful evidence/information to achieve the audit objectives effectively. In addition, the audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence/information by the IS auditor.

12.2 The Information Systems Auditor will require to provide a report in an appropriate form to the designated authority in the organisation upon the completion of the audit work. The audit report will require to, among others, state the scope, objectives, period of coverage and the nature and extent of the audit work performed. Further, the report has to also identify the organisation, the designated authority and the restrictions, if any, on the circulation of the report. In addition, the report has also to state the findings, conclusions, recommendations and any reservations or qualifications that the IS auditor has with respect to the audit.

12.3 Some irregularities may be considered fraudulent activities. The determination of the fraudulent activities depends on the legal definition of fraud. Irregularities include, but are not limited to, the deliberate circumvention of controls with the intent to conceal the perpetuation of fraud, the unauthorised use of the assets or services etc. and the abetting or helping to conceal these types of activities.

12.4 Non-fraudulent irregularities should, among others, include as under:

a) Intentional violations of the established management policy.
b) Intentional violations of the regulatory requirements.
c) Deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole.
d) Gross negligence.
e) Unintentional illegal acts.

The IS auditor will require to consider how to achieve the implementation of the internationally accepted Standards in this regard, use professional judgement in their application to IS auditing and be prepared to justify departure, if any, therefrom.

12.5 The IS auditor should consider defining in the audit charter the responsibilities of the management and audit with respect to the prevention, detection and the reporting of the irregularities, so that these are clearly understood for all audit work. Where these responsibilities are already documented in the organisation's policy against fraud or similar document, the audit charter should include a statement to that effect.

12.6 The Management of the organisation is responsible for the designing, implementation and maintenance of a system of internal controls including the prevention and detection of fraud. The IS auditor is responsible for assessing the risk of fraud and for designing and performing tests, which are appropriate for the nature of the audit assignment and can reasonably be expected to detect the irregularities, which could have a material effect on either the area under audit or the organisation as a whole and the weaknesses in the internal controls, which could result in material irregularities not being prevented or detected.

12.7 An audit cannot guarantee that irregularities will be detected. Even when an audit is appropriately planned and performed, irregularities could go undetected e.g. if there is collusion between the employees, collusion between the employees and the outsiders, or the involvement of the management in the irregularities. The IS auditor should consider documenting this point in the Audit Charter.

12.8 The IS auditor should be reasonably conversant with the subject of fraud to be able to identify the risk factors, which may contribute to the occurrence of fraud. The IS auditor should assess the risk of the occurrence of the irregularities, connected with the area under audit. In preparing this assessment, the IS auditor should consider the under-noted factors :

a) Organisational characteristics such as corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures.
b) History of the organisation.
c) Recent changes in Management, operations or IS systems.
d) Types of assets held or services offered and their susceptibility to irregularities.
e) Strength of the relevant controls. f) Applicable regulatory or legal requirements.

g) History of audit findings from previous audits.

h) The industry and the competitive environment in which the organisation operates.
i) Findings of reviews, carried out outside the scope of audit, such as the findings from the consultants, quality assurance teams or specific management investigations.
j) Findings which have arisen during the day-to-day course of business.
k) The technical sophistication and complexity of the information system(s) supporting the area under audit.
l) Existence of in-house developed/maintained application systems, as compared with the packaged software for core business systems.

12.9 In planning the audit work, appropriate for the nature of the audit assignment, the IS auditor should use the results of the risk assessment to determine the nature, timing and extent of the testing required in order to obtain sufficient audit evidence/information to provide reasonable assurance that the irregularities, which could have a material effect on the area under audit or on the organisation as a whole, will be identified and that the control weaknesses, which would fail to prevent or detect material irregularities, will be identified.
12.10 If irregularities have been detected, the IS auditor should assess the effect of these activities on the audit objectives and on the reliability of the audit evidence/information/ information collected. In addition, the IS auditor should consider whether to continue with the audit work when the effect of the irregularities, thus detected, appears to be so significant that sufficient, reliable audit evidence/information cannot be obtained or the audit evidence/information suggests that the management of the organisation has either participated in or condoned the irregularities.
12.11 If the audit evidence/information indicates that the irregularities could have occurred, the IS auditor should recommend to the management of the organisation that the matter requires to be investigated in detail and that the Management may initiate appropriate actions therefor. If the IS auditor suspects that the management is involved in the irregularity, he/she should identify the appropriate responsible figure in the organisation to whom these conclusions should be reported. If reporting internally proves impossible, the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation. In short, the IS auditor will require to take adequate and considered actions to support the audit findings, conclusions and recommendations.
12.12 If the audit evidence/information indicates that an irregularity could involve an illegal act, the IS auditor should consider seeking legal advice directly or recommending that the management of the organisation may seek legal advice in the matter.
12.13 The detection of the irregularities should be communicated to the appropriate/identified/concerned person/s/authority/ies in the organisation in a timely

manner. The communication should be directed to a level of management above that at which the irregularities might have been suspected to have occurred. In addition, the irregularities should be reported to the Board of Directors, Audit Committee of the Board or Designated Authority, except for matters which are clearly insignificant in terms of both financial effect and indications of control weaknesses.

12.14 The internal distribution of the reports of irregularities should be carefully considered. The occurrence and the effect of irregularities is a sensitive issue and reporting them carries its own risks including further abuse of the control weaknesses as a result of publishing details of them, loss of customers, suppliers and investors when disclosure (authorised or unauthorised) occurs outside the organisation and the loss of key staff and management in the organisation, including those not involved in the irregularity, as the confidence in the management and the future of the organisation falls. In view of the above, the IS auditor should consider reporting the irregularity separately from any other audit issues, if this would assist in controlling the distribution of the report.

12.15 External reporting may be a legal or regulatory obligation. The obligation may apply to the management of the organisation or to the individuals involved in the detection of the irregularities or to both. Where external reporting is required, the report should be approved by the appropriate level of audit management prior to external release and should also be reviewed with the auditee management in advance, unless the applicable regulations or specific circumstances of the audit prevent this. Examples of the specific circumstances, which may prevent obtaining the auditee management's agreement for the purpose, may include, among others, the auditee management's active involvement in the irregularity or the auditee management's passive acquiescence in the irregularity.

12.16 If the auditee management does not agree to the external release of the report, and external reporting is a statutory or regulatory obligation, the IS auditor should consider consulting the audit committee and taking legal counsel about the advisability and risks of reporting the findings outside the organisation.

12.17 The IS auditor, with the approval of the audit management, should submit the report to any appropriate regulators on a timely basis. Where the IS auditor is aware that the management of the organisation is required to report the fraudulent activities to an outside organisation, the IS auditor should formally advise the management of this responsibility. If an irregularity has been detected by an IS auditor, who is not part of the external audit team, the IS auditor, should consider submitting the report to the external auditors on a timely basis.

12.18 Where the audit scope has been restricted, the IS auditor should include an explanation of the nature and the effect of this restriction in the audit report. Such a restriction may occur on account of the following :

a) The IS auditor has been unable to carry out further work, as considered necessary to fulfill the original audit objectives and to support the audit conclusions due to unreliable audit evidence/ information, lack of resources or the restrictions placed on the audit activities by the management of the organisation.

b) Management has not carried out the investigations, as recommended by the IS auditor.

CHAPTER 13
Audit Evidence/Information

13.1 When planning the IS audit work, the IS auditor should take into account the type

of audit evidence/information to be gathered, its use as audit evidence/ information to meet the audit objectives and its varying levels of reliability. Among the things to be considered are the independence and qualifications of the provider of the audit evidence/information. For example, corroborative audit evidence/information from an independent third party can be more reliable than the audit evidence/information from the organization being audited. Physical audit evidence/information is generally more reliable than the representations of an individual.

13.2 The various types of audit evidence/information, which the IS auditor should consider using include as under :

a) Observed processes and existence of physical items
b) Documentary audit evidence/information
c) Representations
d) Analysis

13.2.1 Observed processes and existence of physical items can include observations of activities, property and functions of the information systems such as:

a) Inventory of media in an offsite storage location
b) Computer room security system in operation

13.2.2 Documentary audit evidence/information, recorded on paper or other media, can include:

a) Results of data extractions
b) Records of transactions
c) Program listings
d) Invoices
e) Activity and control logs
f) System development documentation

13.2.3 Representations of those being audited can be audit evidence/information such as:

a) Written policies and procedures
b) System flowcharts
c) Written or oral statements

13.2.4 The results of analyzing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence/information. Examples include:

a) Benchmarking IS performance against other organizations or previous periods.
b) Comparison of error rates between the application transactions and the Users.

13.3 Availability of Audit Evidence/Information :

The IS auditor should consider the time during which the evidence/information exists or is available in determining the nature, timing and extent of Substantive Testing and if applicable, Compliance Testing. For example, the audit evidence/ information processed by Electronic Data Interchange (EDI), Document Image Processing (DIP) and dynamic systems such as spreadsheets etc. may not be retrievable after a specified period of time, if changes to the files are not controlled or the files are not backed up.

13.4 Selection of Audit Evidence/Information :

The IS auditor should plan to use the best audit evidence/information attainable, consistent

with the importance of the audit objective and the time and effort involved in obtaining the audit evidence/information. Where the audit evidence/ information, obtained in the form of oral representations, is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or on other media.

13.5 Nature of Audit Evidence/Information :

Audit evidence/information should be sufficient, reliable, relevant and useful in order to form an opinion or support the IS auditor's findings and conclusions. If in the IS auditor's judgement, the audit evidence/information obtained does not meet these criteria, the IS auditor should obtain additional audit evidence/ information. For example, a program listing may not be adequate audit evidence/ information until other audit evidence/information has been gathered to verify that it represents the actual program used in the production process.

13.6 Gathering Audit Evidence/Information :

Procedures used to gather audit evidence/information vary depending on the information systems being audited. The IS auditor should select the most appropriate procedure for the audit objective. The following procedures should be considered:

a) Inquiry
b) Observation
c) Inspection
d) Confirmation
e) Re-performance
f) Monitoring

The above can be applied through the use of Manual Audit Procedures, Computer-Assisted Audit Techniques or a combination of both. For example, a system, which uses manual control tools to balance data entry operations, might provide audit evidence/information that the control procedure is in place by way of an appropriately reconciled and annotated report. The IS auditor should obtain audit evidence/information by reviewing and testing this report.

Detailed transaction records may be available in machine-readable format requiring the IS auditor to obtain audit evidence/information, using Computer Assisted Audit Techniques.

13.7 Audit Documentation :

Audit evidence/information gathered by the IS auditor should be appropriately documented and organized to support the IS auditor's findings and conclusions.

13.8 Restriction of Scope :

Under those situations, where the IS auditor believes that sufficient audit evidence/information cannot be obtained, the IS auditor should disclose this fact in a manner, consistent with the communication of the audit results.

CHAPTER 14

Audit Documentation

14.1 During the course of IS auditing, the Information Systems Auditor has to obtain sufficient, reliable, relevant and useful evidence/information to achieve the audit objectives

effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence/information. The Information Systems Auditor will require to provide a report, in an appropriate form, to the designated authority upon the completion of the audit work. Further, the audit report should, among others, state the scope, objectives, period of coverage and the nature and extent of the audit work performed. In addition, the report should also identify the organisation, the designated recipients in the organisation and restrictions, if any, on the circulation of the audit report. The report should state, among others, the findings, conclusions and the recommendations of the IS auditor including the reservations or qualifications, if any, which the IS auditor has with respect to the audit. The IS auditor will require to prepare and retain documentation to support the audit work performed. The IS auditor will require to apply internationally accepted IS auditing standards to the performance of the IS audit work, use professional judgement in the application of such standards and should be prepared to justify departure/deviation, if any, therefrom.

14.2 The Information systems audit documentation is the record of the audit work performed and the audit evidence/information supporting the IS auditor's findings and conclusions. The IS audit documentation should :

a) demonstrate the extent up to which the IS auditor has complied with the IS auditing Standards ;
b) assist in the planning, performance and review of audits ;
c) facilitate third-party reviews ;
d) assist in the evaluation of the quality assurance programme relating to the IS auditing function's ;
e) support matters relating to insurance claims, fraud cases and lawsuits ; and
f) assist in the professional development of the staff .

14.3 The IS audit documentation should, among others, include, a record of:

a) the planning and preparation of the audit scope and objectives ;
b) the audit programme;
c) the audit steps performed and audit evidence/information gathered;
d) the audit findings, conclusions and recommendations;
e) any report issued as a result of the audit work ; and
f) Supervisory review

14.4 The extent of the IS auditor's documentation will depend on the needs for a particular audit and should, among others, include such things as :

a) the IS auditor's understanding of the area to be audited and its environment ;
b) the IS auditor's understanding of the information processing systems and the internal control environment;
c) the author and source of the audit documentation and the date of its completion;
d) the audit evidence/information and the source of the audit documentation and the date of completion ; and
e) the auditee's response to recommendations.

14.5 Documentation should include audit information that is required by law, by government regulations and by applicable professional standards. The documentation should be clear, complete and understandable by a reviewer.

14.6 Policies and procedures should be in place to ensure appropriate custody and retention of the documentation that supports audit findings and conclusions for a period of time, sufficient to satisfy legal, professional and organisational requirements.

14.7 Documentation should be organised, stored and secured in a manner appropriate for the media on which it is retained and should continue to be retrievable for a period of time, sufficient to satisfy the above policies and procedures.

CHAPTER 15

Recommendations

Each organisation in the banking and financial sector in the country should formulate its Security Policy on the lines of the guidelines, as set out in the 'Information Systems Security Guidelines' (Annexure). Further, each organisation in the banking and financial sector in the country should conduct Information Systems Audit conforming to the 'Information Systems Audit Policy', as enumerated in this document.

CHAPTER-1 :

1 Auditing is a systematic and independent examination of information systems and their environment to ascertain whether the objectives, set out to be met, have been achieved. The Auditors may not necessarily examine the entire system. They may examine a part or parts of it only. Auditing covers primarily the following broad major areas of activity :

a) gathering of information,

b) comparison of information ; and

c) asking why.

Para 1.1

2 Well planned and structured audit is essential for risk management and monitoring and control of Information Systems in any organisation. **Para 1.2**

3 The frauds, which render the financial statements misleading, require to be brought under the scope of any form of financial audit. **Para 1.4.1**

4 The task of an auditor is to determine whether the financial statements have been fairly presented. To accomplish this, the auditor should establish the audit objectives, design procedures and gather evidence/information, which may corroborate or refute the management's assertions. **Para 1.4.1.1**

5 Compliance with different laws and regulations is monitored by the regulatory authority/ies through Compliance Audit. **Para 1.4.2**

6 IS audit follows a three-phase process, as applicable to Financial Audit and Compliance Audit. The first phase is the audit planning phase, followed by the test of controls phase and finally, the substantive testing phase. In the planning or first phase, an IS auditor should identify various risks and exposures and the security controls, which provide safeguards against these exposures. The tests, which need to be conducted to make the second phase of the audit effective, will require to be planned in detail in the first phase. In the second phase, the security controls are tested. Control activities in an organization are the policies and procedures used to ensure that appropriate actions are taken to deal with the organisation's identified risks. **Para 1.4.3**

7 **I**t is preferable to have the IS audit conducted with the help of suitable external agencies with the required skills and expertise to ensure independent nature of audit. In case of development and deployment of the IT systems by third parties, the IS audit should be conducted by trusted auditor/s with skills and expertise, required for the purpose. **Para 1.4.4**

8 In case of various kinds of audit in a computerized environment, the regulator should issue from time to time, the guidelines, concerning the level of transparency and access to the financial statements, information and information systems. These guidelines will specify not only the key areas of statutory audit, but will also include the areas of operation, where concurrent audit may be necessary. Further, areas should be also identified for off-site and on-site inspection and audit by the regulator. The guidelines should provide for sufficient safeguards to be built in the Information Systems to ensure systemic ruggedness to reduce the risk of cyber and digital crimes like hacking, spamming, unauthorised access and destruction or manipulation of the information and the information systems.

A set of standards, practices and procedures should be worked out for adoption by each organization in the banking and financial sector regarding each and every aspect of computerization including, among others, networking, applications, databases, security features, audit and accounting features. The standards should be generic, open and minimal. The Auditor should keep in view the basic principles in which the computers, networks, databases, applications and security provisions operate in a computerized environment.

The regulator should initially take the help of trusted and independent third party Information Systems Auditors, with suitable skills and expertise for the purpose, alongwith its personnel, for auditing inter-institutional applications. The regulator should also develop a team of expert Information System Auditors in-house for the purpose.

Para 1.5

9 The banks and the financial institutions entities should use Certified Information Systems Auditors (CISA), Certified Information System Security Professionals (CISSP etc. for conduct of IS audit in their respective organisations.

Para 1.6

CHAPTER 2

10 The Management should establish an adequate System of Internal Controls to safeguard all the assets of the organization. During the course of IS audit, the Information Systems Auditor should obtain sufficient, reliable, relevant and useful evidence/information to achieve the audit objectives effectively. The audit findings and conclusions should be supported by appropriate analysis and interpretation of this evidence/information.

Para 2.1

11 Reporting on corporate governance of the information systems will involve auditing at the highest level in the organisation and may cross divisional, functional or departmental boundaries. The management/designated authority in the organization should, therefore, ensure that the audit charter or the engagement letter for the IS auditor clearly states that the scope of IS audit, includes the corporate governance of the information systems and technology togetherwith the reporting line to be used, where corporate

governance issues are identified.
Para 2.2

12 The IS auditor should consider whether the policies, issued, cover all of the appropriate areas for which board-level direction is necessary in order to provide reasonable assurance that the business objectives are met. Such policies on board level direction should be documented ones only and such documented policies shall, among others, include the following :

a) Security Policy
b) Human Resources Policy
c) Data Ownership Policy
d) End-user Computing Policy
e) Copyright Policy
f) Data Retention Policy
g) System Acquisition and Implementation Policy
h) Outsourcing Policy

Para 2.7

13 The IS auditor should consider the position or functions of the IS specialist staff in the organisation and assess whether this is appropriate to enable the organisation to make the best use of IS to achieve its business objectives. The control of the information systems, even in decentralised and end-user run environments, should include segregation of conflicting duties. The IS auditor should assess whether the management of the IS specialists and the nonspecialists with IS responsibilities is adequate to address the risks to the organisation from the errors, omissions, irregularities or illegal acts. **Para 2.11**

CHAPTER 3

14 IS auditor should evaluate the adequacy of the security controls and inform the Management with suitable conclusions and recommendations. The major objectives of IS audit include, among others, the following:

a) Safeguarding of Information System Assets/Resources
b) Maintenance of Data Integrity
c) Maintenance of System Effectiveness
d) Ensuring System Efficiency

Para 3.1

15 The IS audit should cover all the computerized departments/offices of the organisation. The scope of IS audit should include the collection and evaluation of evidence/information to determine whether the Information Systems in use safeguard the assets, maintain data security, integrity and availability, achieve the organizational goals effectively and utilize the resources efficiently. The scope of IS audit should also include the processes for the planning and organization of the Information Systems activity, the processes for the monitoring of such activity and the examination of the adequacy of the organization and management of the IS specialist staff and the non-specialists with IS responsibilities to address the exposures of the organization.

Para 3.2

CHAPTER 5

16 The IS auditors should utilize the manual procedures, when they are more effective than the other alternatives or when the procedures cannot be partially or fully automated. He/She should also use computer assisted procedures known as Computer Assisted Audit Techniques (CAATs) because they permit the IS auditors to switch from the procedures based on limited, random and statistical samples of records in a file to a procedure that includes every record in a file.

Para 5.1

17 Audit activity is broadly divided into 5 major steps for the convenience and effective conduct of audit.

a) Planning of Audit
b) Tests of Controls
c) Tests of Transactions
d) Tests of Balances
e) Completion of Audit

Para 5.2

CHAPTER 6

18 The responsibility, authority and accountability of the information systems audit function, both internal and external, should be appropriately documented in an audit charter or engagement letter, defining the responsibility, authority and accountability of the IS audit function. The IS auditor should determine how to achieve the implementation of the applicable IS audit standards, use professional judgement in their application and be prepared to justify any departure therefrom.

The IS auditor should have a clear mandate from the organization to perform the IS audit function. This mandate is ordinarily documented in an audit charter, which should be formally accepted by the IS auditor. The audit charter, for the audit function as a whole, should include the IS audit mandate.

CHAPTER 7

19 The IS auditor should follow the guidelines for planning the information systems audit work. These guidelines should cover the planning process, the identification of the levels of planning and the documentation of the work to be performed by the IS auditor. These guidelines should also set out how the IS auditor will comply with the internationally accepted standards.

CHAPTER 8

20 The specialised nature of the Information Systems (IS) auditing and the skills, necessary to perform such audit, require standards that apply specifically to IS auditing. Such standards will require to be internationally accepted standards only. This will ensure that the IS auditor performs auditing, conforming to the minimum level of acceptable performance and meeting the required professional responsibilities.

Para 8.1

21 The IS auditor should prepare the procedure including the information on how to meet the Standards while performing the IS auditing work. However, the procedure shall not set the requirements for IS auditing.

Para 8.3

22 IS auditing should be performed by personnel with the required expertise and skills such as Certified Information Systems Auditor, Certified Information Systems Security Professionals etc.

Para 8.4

23 Major areas, which should be IS audited, are broadly as under:

a) Safeguarding of Assets
b) Data Integrity
c) System Effectiveness
d) System Efficiency
e) Organization and Administration
f) Business Continuity Operations

Para 8.6)

CHAPTER 9

24 The IS auditor should design and select an audit sample and evaluate the sample results. Appropriate sampling and evaluation will meet the requirements of "sufficient, reliable, relevant and useful evidence/information" and "supported by appropriate analysis". The IS auditor should select the techniques, which result in a representative sample statistically for performing the Compliance or Substantive Testing. Examples of Compliance Testing of the internal controls, where sampling could be considered, should, among others, include user access rights, program change control procedures, documentation procedures, program documentation, follow up of exceptions, review of logs, software license audit etc. Examples of the Substantive Tests, where sampling could be considered, should, among others, include re-performance of a complex calculation (e.g. calculation of interest) on a sample of accounts, sample of transactions, supporting documentation etc.

CHAPTER 10

25 The security measures for safeguarding the information resources should include the identification and assessment of risks and the development of proper controls to offset/reduce possible threats.

Para 10.4

26 The Information System should safeguard its assets and maintain data integrity. It should help in achieving the organization's goals. A secure information system should have established comprehensive procedures and controls, which are backed by commitment from the Management of the organisation. It is required to periodically monitor that these procedures and controls are in place and operational to effectively ensure that the information stored in these systems continues to be dependable. Periodical monitoring is achieved by IS audit. IS audit is a process of collecting and evaluating information to determine whether a computer system could :

a) safeguard its assets (hardware, software and data) through adoption of adequate security control measures ;

b) maintain data integrity ;
c) achieve goals of the organization effectively ; and
d) result in efficient use of the available Information System resources.

Para 10.5

CHAPTER 11

27 The IS audit differs from the traditional audit in the sense that it requires adequate knowledge of computer systems in addition to the basic concepts of normal auditing. Information Technology is rapidly changing. It is essential that the IS auditors keep themselves abreast of the latest systems and techniques of IS auditing. The IS auditors should equip themselves with the under-noted information to successfully perform IS auditing :

a) A general understanding of the operating systems in use.
b) Thorough knowledge of application software in use.
c) Knowledge of the automated operations, methods of storing and retrieval of data and controls used in the systems.
d) Knowledge of the methodology used in data processing.
e) IS auditors for auditing complex systems require substantial knowledge about the development, implementation and operation of the systems. A thorough understanding of various controls in the development of systems, maintenance of data and network management is essential.
f) An understanding of the emerging technologies, capacity to determine their impact on controls, ability to change audit procedures suitably and to develop evidence/information collection tools and techniques.
g) IS auditors, to be engaged, should maintain technical proficiency and keep themselves abreast of the current changes in the procedures, technologies adopted and the functions computerized by the organisations in the banking and financial sector.
h) Ability to identify general security measures including risk analysis.
i) Capabilities to render constructive disaster assessment.
j) Sound knowledge of the organisation's accounting practice and record keeping requirements.
k) Ability to investigate thoroughly and to document the investigation work.
l) The audit process requires initiative, thoroughness and tact while addressing an audit assignment.
m) IS audit calls for understanding and the capabilities to analyze and offer constructive comments on the Information Systems Security and Controls.
n) All material irregularities are required to be reported and the IS auditor should report all the unpleasant findings.
o) The IS auditors should be aware of the situations where too much trust has been placed on one individual. One person acting alone could commit an error willfully or defraud the organisation. This is important in those transactions, which are perceived to be of high risk.
p) Capacity to plan and supervise IS audit to assure that the audit meets the desired objectives, as set out in the audit assignment, efficiently.
q) Knowledge of the basics in computer programming would help in having clarity of approach.

Para 11.2

CHAPTER 12

28 The Information Systems Auditor should plan the information systems audit work to address the audit objectives and to comply with internationally accepted professional auditing standards. Further, during the course of IS auditing, the Information Systems Auditor should obtain sufficient, reliable, relevant and useful information to achieve the audit objectives effectively. In addition, the audit findings and conclusions should be supported by appropriate analysis and interpretation of this information by the IS auditor. **Para 12.1**

CHAPTER 13

29 When planning the IS audit work, the IS auditor should take into account the type of audit evidence/information to be gathered, its use as such evidence

109 information to meet the audit objectives and its varying levels of reliability. Among the things to be considered are the independence and qualifications of the provider of the audit information. For example, corroborative audit information from an independent third party can be more reliable than audit evidence/information from the organization being audited. Physical audit evidence/information is generally more reliable than the representations of an individual.

Para 13.1

30 The various types of audit information, which the IS auditor should consider using, include as under :

a) Observed processes and existence of physical items
b) Documentary audit information
c) Representations
d) Analysis

Para 13.2

CHAPTER 14

31 During the course of IS auditing, the Information Systems Auditor should obtain sufficient, reliable, relevant and useful information to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this information. The Information Systems Auditor should provide a report, in an appropriate form, to the designated authority upon the completion of the audit work. Further, the audit report should, among others, state the scope, objectives, period of coverage and the nature and extent of the audit work performed. In addition, the report should also identify the organisation, the designated recipients in the organisation and restrictions, if any, on the circulation of the audit report. The report must state, among others, the findings, conclusions and the recommendations of the IS auditor including the reservations or qualifications, if any, which the IS auditor has with respect to the audit. The IS auditor should prepare and retain documentation to support the audit work performed. The IS auditor should apply internationally accepted IS auditing standards to the performance of the IS audit work, use professional judgment in the application of such standards and should be prepared to justify departure/deviation, if any, therefrom. **Para**

14.1

GLOSSARY OF TERMS

Appearance : The act of giving the idea or impression of being or doing something.

Appearance of Independence : Behavior adequate to meet the situations occurring during audit work (interviews, meetings, reporting, etc.). The IS auditor should be aware that appearance of independence depends upon the perceptions of others and can be influenced by improper actions or associations.

Application Acquisition Review : An evaluation of an application system, being acquired or evaluated, which considers, as under, whether :

a) appropriate controls are designed into the application system;
b) the application system will process information in a complete, accurate and reliable

manner;
c) the application system will function as intended;
d) the application system will function in compliance with any applicable statutory provisions; and
e) the application system is acquired in compliance with the established system acquisition process.

Application Controls relate to the transactions and the standing data, pertaining to each computer-based application system and are, therefore, specific to each such application. The objectives of application controls, which may be manual or programmed, are to ensure the completeness and accuracy of the records and the validity of the entries made therein, resulting from both manual and programmed processing. Examples of application controls include data input validation, agreement of batch totals and encryption of data transmitted.

Application Development Review : An evaluation of an application system under development which considers, as under, whether :
a) appropriate controls are designed into the system;
b) the application system will process information in a complete, accurate and reliable manner;
c) the application system will function as intended;
d) the application system will function in compliance with any applicable statutory provisions; and
e) the application system is developed in compliance with the established systems development life cycle process.

Application Implementation Review : An evaluation of any part of an implementation project (e.g. project management, test plans, user acceptance testing procedures).

Application Maintenance Review : An evaluation of any part of a project to perform maintenance on an application system (e.g. project management, test plans, user acceptance testing procedures).

Application Software Tracing and Mapping : Specialised tools that can be used to analyse the flow of data through the processing logic of the application software and document the logic, paths, control conditions and processing sequences. Both the command language or job control statements and the programming language can be analysed. This technique includes program/system, mapping, tracing, snap shots, parallel simulations and code comparisons.

Application System : An integrated set of computer programs, designed to serve a particular function that has specific input, processing and output activities (e.g. general ledger, manufacturing resource planning, human resource management).

Attitude : Way of thinking, behaving, feeling, etc.

Audit Accountability : Performance measurement of service delivery including cost, timeliness and quality against agreed service levels.

Audit Authority : A statement of the position within the organisation, including lines of reporting and the rights of access.

Audit Charter : A document which defines the IS audit function's responsibility, authority and accountability.

Audit Evidence/Information : The Information Systems Auditor (IS auditor) gathers evidence/information in the course of performing an IS audit. The information used by the IS auditor to meet audit objectives is referred to as audit evidence/information.

Audit Expert Systems : Expert or decision support systems that can be used to assist the IS auditors in the decision-making process by automating the knowledge of the experts in the field. This technique includes automated risk analysis, system software, and Control Objectives software packages.
Audit Programme : A series of steps to achieve an audit objective.
Audit Responsibility : The roles, scope and objectives, documented in the service level agreement, between the management of the organisation and the IS auditor.
Audit Risk : The risk of giving an incorrect audit opinion.
Audit Sampling : The application of audit procedures to less than 100% of the items within a population to obtain audit evidence/information about a particular characteristic of the population.
CAATs (Computer Assisted Audit Techniques) : Any automated audit techniques, such as the generalised audit software, utility software, test data, application software, tracing and mapping and audit expert systems.
Compliance Testing : Tests of control, designed to obtain audit evidence/ information on both the effectiveness of the controls and their operation during the audit period.
Control Risk : The risk that an error, which could occur in an audit area and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system.
Corporate Governance : The system by which organisations are directed and controlled. Boards of directors are responsible for the governance of their organisations.
Detailed IS Controls : Controls over the acquisition, implementation, delivery and support of IS systems and services. They are made up of application controls plus those general controls not included in pervasive controls.
Detection Risk : The risk that the IS auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors.
Due Care: Diligence which a person would exercise under a given set of circumstances.
Due Professional Care : Diligence which a person, who possesses a special skill, would exercise under a given set of circumstances.
Embedded Audit Module : Integral part of an application system that is designed to identify and report specific transactions or other information based on predetermined criteria. Identification of reportable items occurs as part of real-time processing. Reporting may be real-time on-line or may use store and forward methods. Also known as Integrated Test Facility or Continuous Auditing Module.
Engagement Letter : Formal document which defines the IS auditor's responsibility, authority and accountability for a specific assignment.
Error : Control deviations (compliance testing) or misstatements (substantive testing).
Error Risk : The risk of errors occurring in the area being audited.
Exposure : The potential loss to an area/organization due to the occurrence of an adverse event.
General Controls : Controls, other than application controls, which relate to the environment within which the computer-based application systems are developed, maintained and operated and which are, therefore, applicable to all the applications. The objectives of general controls are to ensure the proper development and implementation of the applications and the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples

of general controls include the development and implementation of an IS strategy and an IS security policy, the organisation of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

Generalised Audit Software : A computer program or series of programs, designed to perform certain automated functions. These functions include reading computer files, selecting data, manipulating data, sorting data, summarising data, performing calculations, selecting samples and printing reports or letters in a format, specified by the IS auditor. This technique includes software acquired or written for audit purposes and software embedded in production systems.

Independence : Self-governance, freedom from conflict of interest and undue influence. The IS auditor should be free to make his/her own decisions, not influenced by the organisation being audited and its people (managers and employers).

Independent Appearance : The outward impression of being self-governing and free from conflict of interest and undue influence.

Independent Attitude : Impartial point of view which allows the IS auditor to act objectively and with fairness.

Inherent Risk : The susceptibility of an audit area/organization to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls.

Internal Control : The policies, procedures, practices and organisational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

Irregularities : Intentional violations of established management policy or regulatory requirements, deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole, gross negligence or unintentional illegal acts.

Materiality : An expression of the relative significance or importance of a particular matter in the context of the organisation as a whole.

Objectivity : The ability to exercise judgement, express opinions and to recommend with impartiality.

Outsourcing : A formal agreement with a third party to perform an IS function for an organisation.

Pervasive IS Controls : Those general controls which are designed to manage and monitor the IS environment and which, therefore, affect all IS-related activities.

Population : The entire set of data from which a sample is selected and about which the IS auditor wishes to draw conclusions.

Professional Competence : Proven level of ability, often linked to qualifications issued by relevant professional organisations and compliance with their codes of practice and standards.

Project Sponsor : The person responsible for high-level decisions such as changes to the scope and/or budget of the project and whether or not to implement.

Project Team : Group of people responsible for a project, whose terms of reference may include the development, acquisition, implementation or maintenance of an application system. The team members may include line management, operational line staff, external contractors and IS auditors.

Reasonable Assurance : A level of comfort, short of a guarantee but considered adequate, given the costs of the control and the likely benefits achieved.

Relevant Audit Evidence/Information : Audit evidence/information is relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions, it is used to support.

Reliable Audit Evidence/Information : Audit evidence/information is reliable if, in the IS auditor's opinion, it is valid, factual, objective and supportable.

Risk : The possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems.

Risk Assessment : A process used to identify and evaluate risks and their potential effect.

Sampling Risk : The probability that the IS auditor has reached an incorrect conclusion because an audit sample, rather than the whole population, was tested. While sampling risk can be reduced to an acceptably low level by using an appropriate sample size and selection method, it can never be eliminated.

Service Level Agreement (SLA) : Defined minimum performance measures at or above which the service delivered is considered acceptable.

Service Provider : The organisation which provides the outsourced service.

Service User : The organisation which uses the outsourced service.

Substantive Testing : Tests of detailed activities and transactions or analytical review tests, designed to obtain audit evidence/information on the completeness, accuracy or existence of those activities or transactions during the audit period.

Sufficient Audit Evidence/information : Audit evidence/information is sufficient if it is adequate, convincing and would lead another IS auditor to form the same conclusions.

Systems Acquisition Process : The procedures established to purchase application software or an upgrade, including evaluation of the supplier's financial stability, track record, resources and references from existing customers.

Systems Development Life Cycle Process : An approach used to plan, design, develop, test and implement an application system or a major modification to an application system.

Test Data : Simulated transactions that can be used to test processing logic, computations and controls actually programmed in computer applications. Individual programs or an entire system can be tested. This technique includes Integrated Test Facilities (ITFs) and Base Case System Evaluations (BCSEs).

Useful Audit Evidence/Information : Audit evidence/information is useful if it assists the IS auditors in meeting their audit objectives.

Utility Software : Computer programs provided by a computer hardware manufacturer or software vendor and used in running the system. This technique can be used to examine processing activity, test programs and system activities and operational procedures, evaluate data file activity and analyse job accounting data.

REFERENCES

1. Internal and External Audits Comptroller's Handbook July 2000.
2. Information Systems Auditing and Assurance – James A Hall, South Western College Publishing.
3. Network Auditing – Gordon E. Smith, John Wiley and Sons.
4. Taxmann's Bank Audits Practice Manual – Nitant P Trilokekar
5. The Quality Auditor's Handbook – N L Freeman, Prentice Hall.
6. EDI Control and Audit – Albert J Marcella and Sally Chan, Artec House.
7. Standard for Auditing Computer Applications – Martin A Krist, Auerbach.

8. Financial Accounting – Meigs & Meigs and Bettner and Whittington, Irvin McGraw Hill.
9. The Information Systems Audit Manual, prepared by the 'Working Group on the introduction of Information Systems Audit in Reserve Bank of India'.
10. Guidelines for Information Systems Audit by the Information Systems Audit and Control Association & Information Systems Audit and Control Foundation.
11. Information Technology Act, 2000 dated the 17th October, 2000 –Government of India
12. Information Technology (Certifying Authorities) Rules, 2000 dated the 17th October, 2000 – Government of India