

SYSTEM AUDIT

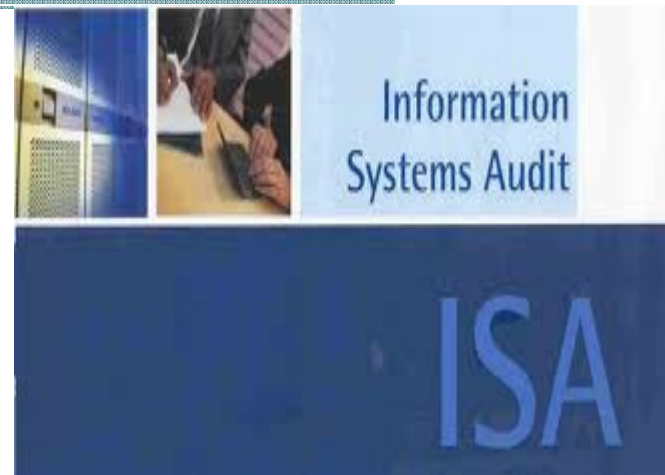
WIRC OF ICAI

DATE: 23RD AUGUST,2014.

BY:

JIGNESH NAGDA

CHARTERED ACCOUNTANT



CONTENTS

- Evolution of I.T. In banking sector
- Recent Developments in Banking Sector
- Need for Information System Audit
- Risk Involved in CIS Environment
- Meaning of systems audit
- Objectives of Information System Audit
- Core Banking Solution
- Audit Methodology
- Information System Process
- Scope of Audit



EVOLUTION OF I.T. IN BANKING SECTOR



- The IT saga in Indian Banking commenced from the mid eighties of the twentieth century when the Reserve Bank took upon itself the task of promoting automation in banking to improve customer service, book keeping, MIS and productivity. This role played by the Reserve Bank has continued over the years.
- Introduction of MICR based cheque processing – a first for the region, during the years 1986-88

EVOLUTION OF I.T. IN BANKING SECTOR

- Computerisation of branches of banks – in the late eighties with the introduction of ledger posting machines (LPMs), advanced ledger posting machines (ALPMs), which have paved the way for installation of Core Banking solutions.
- The setting up of the Institute for Development and Research in Banking Technology (IDRBT), Hyderabad in the mid nineties, as a research and technology centre for the Banking sector;

EVOLUTION OF I.T. IN BANKING SECTOR

- The commissioning in 1999, of the Indian Financial Network as a Closed User Group. The network supports applications having features such as Public Key Infrastructure (PKI) which international networks such as S.W.I.F.T. are now planning to implement ;
- Commencement of Certification Authority (CA) functions of the IDRBT for ensuring that electronic banking transactions get the requisite legal protection under the Information Technology Act, 2000;

EVOLUTION OF I.T. IN BANKING SECTOR

- Ensuring Information Systems Audit (IS Audit) in the banks for which detailed guidelines relating to IS Audit were formulated and circulated;
- Enabling IT based delivery channels which enhance customer service at banks, in areas such as cash delivery through shared Automated Teller Machines (ATMs), card based transaction settlements etc.;

EVOLUTION OF I.T. IN BANKING SECTOR

- Providing detailed specifications to banks on the configuration of systems relating to critical inter-bank payment system applications such as Real Time Gross Settlement (RTGS) System, Negotiated Dealing System (NDS), Centralised Funds Management System (CFMS) etc.
- Setting up connectivity of all clearing houses of the country so as to enable the introduction of the National Settlement System (NSS).

EVOLUTION OF I.T. IN BANKING SECTOR

- The Reserve Bank has set out its Vision document which provides a bird's eye view of the plans for IT development in the medium term, with the required focus on corporate governance. The Vision document has been divided into four major focus areas as follows:
 - IT for regulation and supervision
 - IT and IDRBT
 - IT for the Financial Sector
 - IT for Government related functions

Recent Developments in Banking Sector

- **Society for Worldwide Inter-bank Financial Telecommunications (SWIFT):**



- SWIFT, as a co-operative society was formed in May 1973 with 239 participating banks from 15 countries with its headquarters at Brussels.
- It started functioning in May 1977. RBI and 27 other public sector banks as well as 8 foreign banks in India have obtained the membership of the SWIFT.

Recent Developments in Banking Sector

- SWIFT provides have rapid, secure, reliable and cost effective mode of transmitting the financial messages worldwide. At present more than 3000 banks are the members of the network. To cater to the growth in messages, SWIFT was upgrade in the 80s and this version is called SWIFT-II.
- Banks in India are hooked to SWIFT-II system. SWIFT is a method of the sophisticated message transmission of international repute. This is highly cost effective, reliable and safe means of fund transfer.

Recent Developments in Banking Sector

- This network also facilitates the transfer of messages relating to fixed deposit, interest payment, debit-credit statements, foreign exchange etc.
- This service is available throughout the year, 24 hours a day.
- This system ensure against any loss of mutilation against transmission.

Recent Developments in Banking Sector

- It serves almost all financial institution and selected range of other users
- It is clear from the above benefit of SWIFT that it is very beneficial in effective customer service. SWIFT has extended its range to users like brokers, trust and other agents.

Recent Developments in Banking Sector

Automated Teller Machine (ATM):



- ATM is an electronic machine, which is operated by the customer himself to make deposits, withdrawals and other financial transactions.
- ATM is a step in improvement in customer service. ATM facility is available to the customer 24 hours a day. The customer is issued an ATM card. This is a plastic card, which bears the customer's name. This card is magnetically coded and can be read by this machine.
- .

Recent Developments in Banking Sector

- Each cardholder is provided with a secret personal identification number (PIN). When the customer wants to use the card, he has to insert his plastic card in the slot of the machine.
- After the card is recognized by the machine, the customer enters his personal identification number. After establishing the authentication of the customer, the ATM follows the customer to enter the amount to be withdrawn by him

Recent Developments in Banking Sector

- After processing that transaction and finding sufficient balances in his account, the output slot of ATM give the required cash to him. When the transaction is completed, the ATM ejects the customer's card.



- **Electronic Clearing Service:**
- In 1994, RBI appointed a committee to review the mechanization in the banks and also to review the electronic clearing service.

Recent Developments in Banking Sector

- The committee recommended in its report that electronic clearing service-credit clearing facility should be made available to all corporate bodies/Government institutions for making repetitive low value payment like dividend, interest, refund, salary, pension or commission.
- It was also recommended by the committee Electronic Clearing Service-Debit clearing may be introduced for pre-authorized debits for payments of utility bills, insurance premium and installments' to leasing and financing companies.

Recent Developments in Banking Sector

- RBI has been necessary step to introduce these schemes, initially in Chennai, Mumbai, Calcutta and New Delhi.
- **Bank net:**
- Bank net is a first national level network in India, which was commissioned in February 1991.
- It is communication network established by RBI on the basis of recommendation of the committee appointed by it under the chairmanship of the executive director T.N.A. Lyre. Bank net has two phases: Bank net-I and Bank net- II.

Recent Developments in Banking Sector

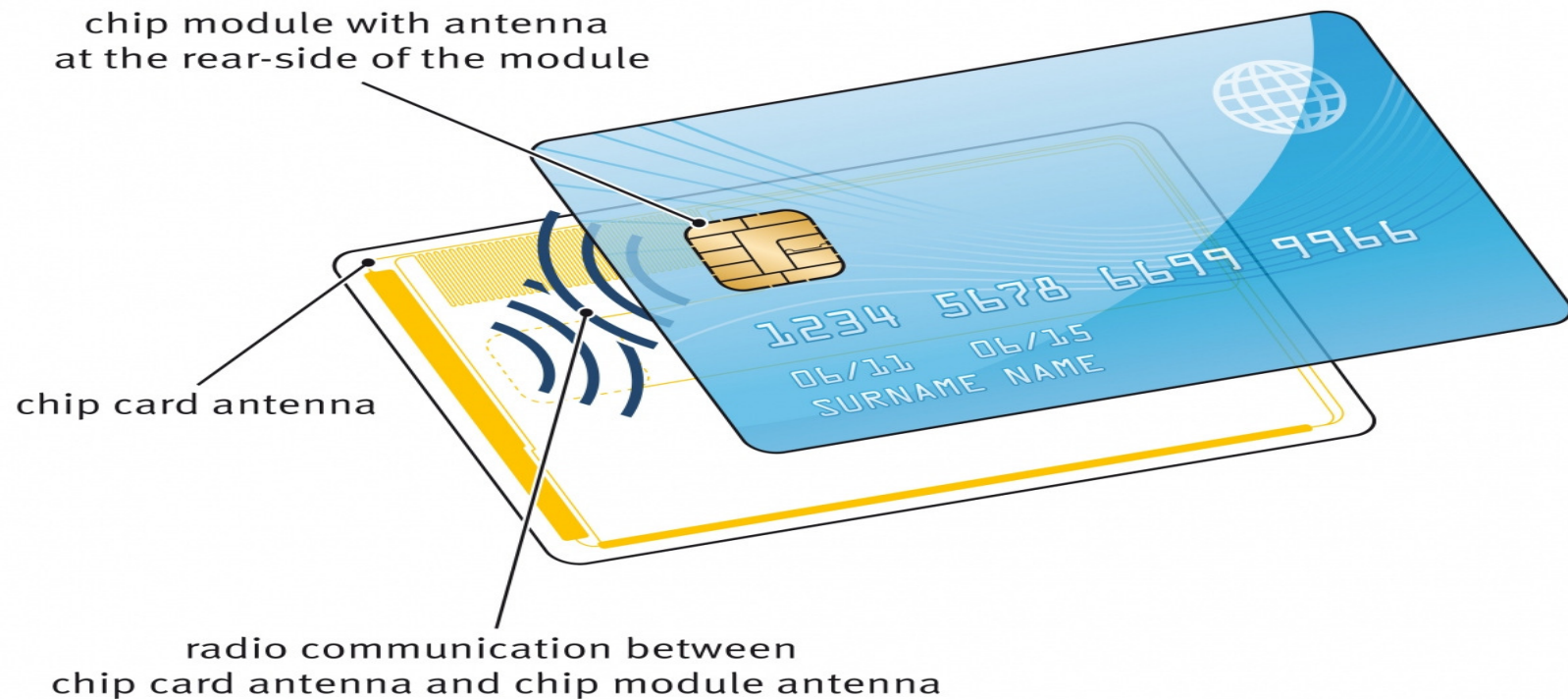
- **Areas of Operation and Application of Bank net:**
- The message of banking transaction can be transferred in the form of codes from the city to the other.
- Quick settlement of transactions and advices.
- Improvement in customer service-withdrawal of funds is possible from any member branch.

Recent Developments in Banking Sector

- Easy transfer of data and other statements to RBI.
- Useful in foreign exchange dealings.
- Access to SWIFT through Bank net is easily possible.

Recent Developments in Banking Sector

- **Chip Card:**



Recent Developments in Banking Sector

- The customer of the bank is provided with a special type of credit card which bears customer's name, code etc.
- The credit amount of the customer account is written on the card with magnetic methods. The computer can read these magnetic spots.

Recent Developments in Banking Sector

- When the customer uses this card, the credit amount written on the card starts decreasing. After use of number of times, at one stage, the balance becomes nil on the card.
- At that juncture, the card is of no use. The customer has to deposit cash in his account for re-use of the card. Again the credit amount is written on the card by magnetic means.

Recent Developments in Banking Sector



Phone Banking:

- Customers can now dial up the bank's designed telephone number and he by dialling his ID number will be able to get connectivity to bank's designated computer.
- The software provided in the machine interactive with the computer asking him to dial the code number of service required by him and suitably answers him.
- By using Automatic voice recorder (AVR) for simple queries and transactions and manned phone terminals for complicated queries and transactions, the customer can actually do entire non-cash relating banking on telephone: Anywhere, Anytime.

Recent Developments in Banking Sector

- **Tele-banking:**



- Tele banking is another innovation, which provided the facility of 24 hour banking to the customer. Tele-banking is based on the voice processing facility available on bank computers.
- The caller usually a customer calls the bank anytime and can enquire balance in his account or other transaction history. In this system, the computers at bank are connected to a telephone link with the help of a modem.

Recent Developments in Banking Sector

- Voice processing facility provided in the software. This software identifies the voice of caller and provides him suitable reply. Some banks also use telephonic answering machine but this is limited to some brief functions.
- This is only telephone answering system and now Tele-banking. Tele banking is becoming popular since queries at ATM's are now becoming too long

Recent Developments in Banking Sector

Internet Banking:



- Internet banking enables a customer to do banking transactions through the bank's website on the Internet.
- It is a system of accessing accounts and general information on bank products and services through a computer while sitting in its office or home.
- This is also called virtual banking. It is more or less bringing the bank to your computer.

Recent Developments in Banking Sector

- In traditional banking one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts etc. but internet banking has changed the way of banking. Now one can operate all these type of transactions on his computer through website of bank. All such transactions are encrypted; using sophisticated multi-layered security architecture, including firewalls and filters. One can be rest assured that one's transactions are secure and confidential.

Recent Developments in Banking Sector



Mobile Banking:

- Mobile banking facility is an extension of internet banking.
- The bank is in association with the cellular service providers offers this service. For this service, mobile phone should either be SMS or WAP enabled. These facilities are available even to those customers with only credit card accounts with the bank.

Recent Developments in Banking Sector

Voice Mail:

- Talking of answering systems, there are several banks mainly foreign banks now offering very advanced touch tone telephone answering service which route the customer call directly to the department concerned and allow the customer to leave a message for the concerned desk or department, if the person is not available



Recent Developments in Banking Sector

- **Any where Banking:**
- With expansion of technology, it is now possible to obtain financial details from the bank from remote locations.

Basic transaction can be effected from faraway places. Automated Teller Machines are playing an important role in providing remote services to the customers.

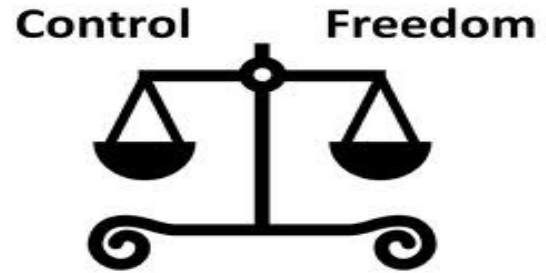
-



Recent Developments in Banking Sector

- Withdrawals from other stations have been possible due to inter-station connectivity of ATM's.
- The Rangarajan committee had also suggested the installation of ATM at non-branch locations, airports, hotels, Railway stations, Office Computers, Remote Banking is being further extended to the customer's office and home.

Need for Information System Audit



- Information systems are very important for running any large business. Earlier computer systems were used to merely record business transactions, but now they are actually used for taking business decisions for the enterprise.
- They are complex and have many components coming together to make a complete business solution.

Need for Information System Audit

- Their usage into accounting systems changed the way data was stored, retrieved and controlled. In such a complex scenario management and business managers are concerned about information systems.

Need for Information System Audit

- IT auditing is the future of the accounting profession. In today's world, company dynamics / financial state is determined by the use of computers.
- The rise in information technology usage is rapid and just be utilized for organizational success.

Need for Information System Audit

- The role IT auditors play may be unknown to most but it impacts the lives of all.
- IT auditing adds security, reliability and accuracy to the information systems.
- Without IT auditing, we would be unable to safely shop on the internet or control our identities. As history continues, we will continue to see the rise of this up and coming profession.

Need for Information System Audit

Information Technology has changed the business environment in the following significant ways:

1. It has increased the ability to capture, store, analyze and process tremendous amounts of data and information and has impacted what one can do in business in terms of information and as a business enabler.



Need for Information System Audit

- IS has empowered the business decision-maker many times over. It also has become a primary enabler to various production processes and service processes.
- It has become a critical component of business processes.
- There is a residual effect in that the increased use of technology has resulted in increased budgets, increased success and failures and increased awareness of the need to control.

Need for Information System Audit

- 2. Technology has impacted controls significantly. While control objectives have in large part remained constant, except for some that are technology-specific, technology changes have altered the way systems should be controlled.
- Safeguarding assets as a control objective remains the same, whether manual or automated. However, the manner through which the control objectives are met is decisive.

Need for Information System Audit

3. Technology has impacted the auditing profession in terms of how audits are performed (information capture and analysis, control concerns) and the knowledge required to draw conclusions regarding operational or system effectiveness, efficiency and integrity, and reporting integrity.
- Initially, the impact was focused on dealing with a changed processing environment. As the need for auditors with specialized skills regarding technology grew, so did the beginning of the information systems auditing profession.

Need for Information System Audit

- The first use of a computerized accounting system was at General Electric in 1954. During the period of 1954 to the mid-1960s, the auditing profession was still auditing around the computer.
- At this time only, mainframe computers were used and few people had the skills and abilities to program computers. This began to change in the mid-1960s with the introduction of new, smaller and less expensive machines.
- This increased the use of computers in businesses and with it came the need for auditors to become familiar with EDP concepts in business.



Need for Information System Audit

- Along with the increase in computer use, came the rise of different types of accounting systems. The formation and rise in popularity of the internet and E-commerce have had significant influences on the growth of IT audit.
- The internet influences the lives of most of the world and is a place of increased business, entertainment and crime.
- IT auditing helps organizations and individuals on the internet find security while helping commerce and communications to flourish.

Need for Information System Audit

- Computer based systems audit functions do not undermine the importance of traditional internal controls such as separation of duties but are implemented differently. Compared to the manual internal control systems, collecting of evidence on the reliability of internal controls is often more complex in the computer based information systems. Computer controls are often more critical than manual controls.
- Evaluation of the reliability of the controls in computer systems is often more complex that in the manual systems. Greater numbers of more complex controls need to be considered. Other sciences such as traditional auditing, computer science, management and behavioural science are the basis of the porinciples and practice of information systems auditing.

Risk Involved in CIS Environment

- Lack of Transaction Trails – e.g. Evidence of application of interest on deposit & advances – System Generated Entries
- Uniform Processing of Transactions- i.e. If Error occurs it applies to all transaction
- Lack of segregation of incompatible functions – i.e. Same person makes-checks, Same person deals with customer & create the Account masters/parameters



Risk Involved in CIS Environment

- Potential for Errors & Irregularities-
 - Due to invisibility of data.
 - No visible evidence for unauthorized access/alter to data (ledger written with pencils)
 - Errors in System Handled transaction – No human intervention/observation hence remains undetected
 - Errors in Designing or modification of Programs can remain undetected.

Risk Involved in CIS Environment

- Manual Controls in such system are dependent upon the Computer Generated Report. Any Error in Report will affect even the manual control.
- CIS related Fraud
 - Unauthorized use – to modify, copy or use the data
 - Internet fraud
 - System Fraud



MEANING OF SYSTEMS AUDIT

- Reserve Bank of India constituted a 'Working Group for Information Systems Security for the Banking and Financial Sector' in October 2001 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'.

MEANING OF SYSTEMS AUDIT

- They have defined Information Systems as ***“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”.***

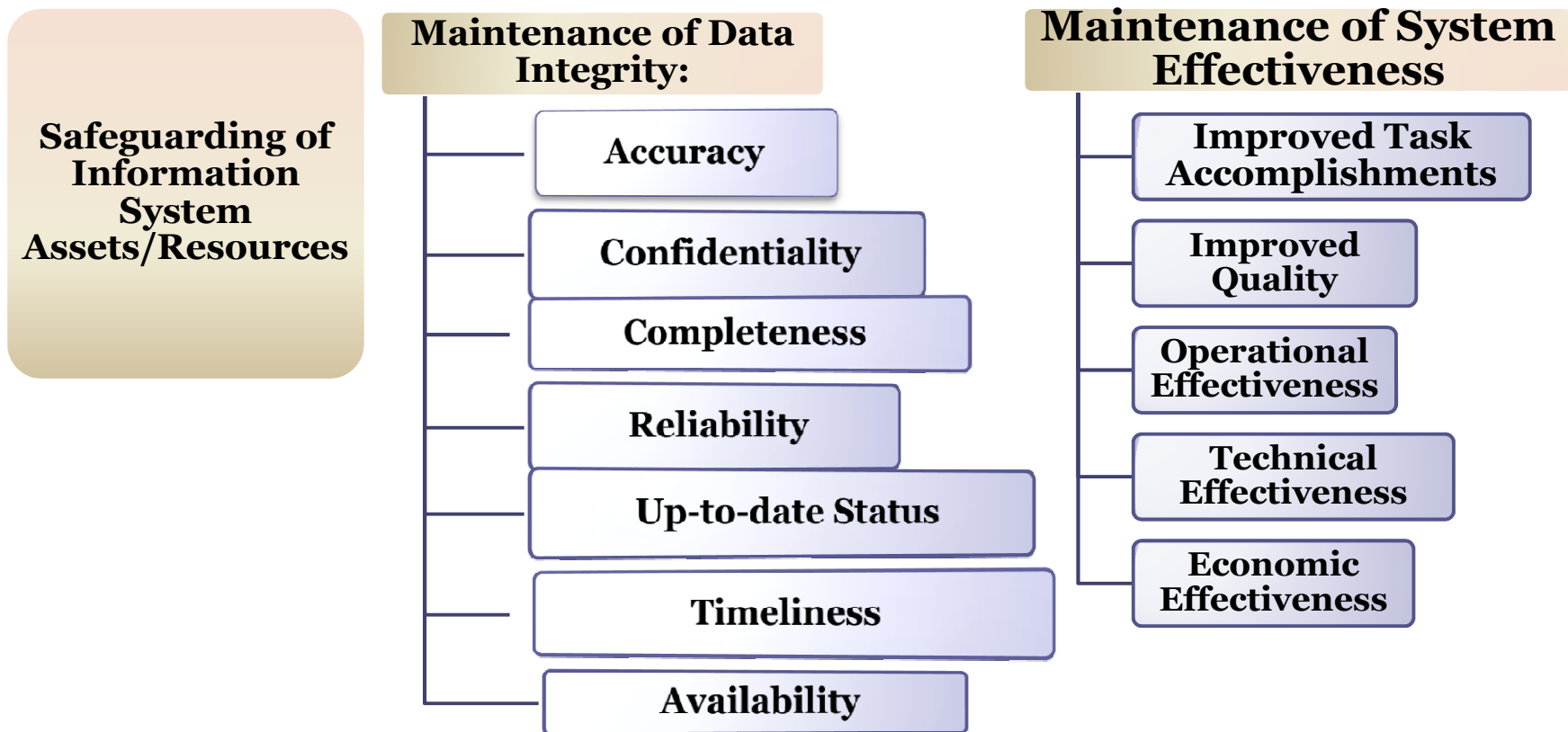


BASIC OF SYSTEM AUDIT

IS Auditing covers primarily the following broad major areas of activity :

- a) gathering of information
 - b) comparison of information and
 - c) asking why
- **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.

OBJECTIVES OF INFORMATION SYSTEM AUDIT



OBJECTIVES OF ISA

- ***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.

OBJECTIVES OF ISA

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.

OBJECTIVES OF ISA

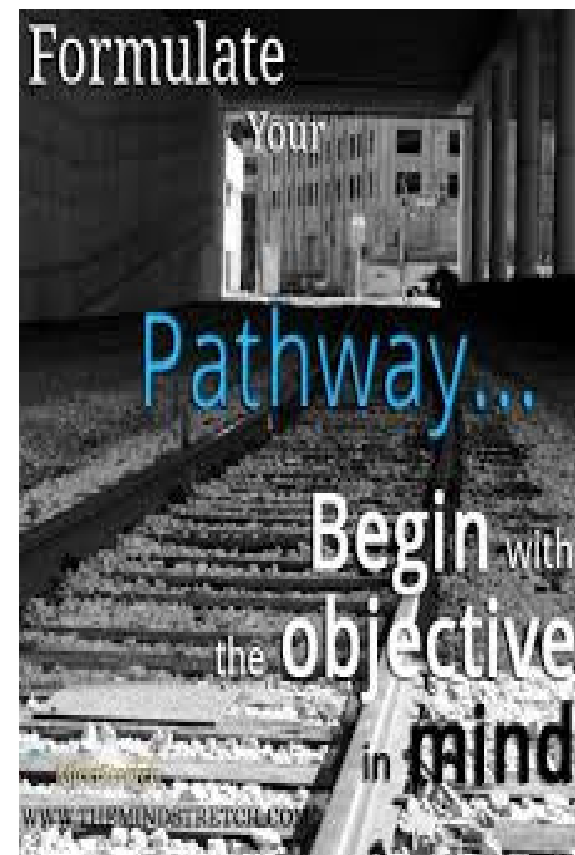
- e) Contribute effectively towards the minimization of computer abuses/ crimes by suggesting steps for removing any laxity observed in the physical and logical controls.

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

OBJECTIVES OF ISA

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.



Core Banking Solution

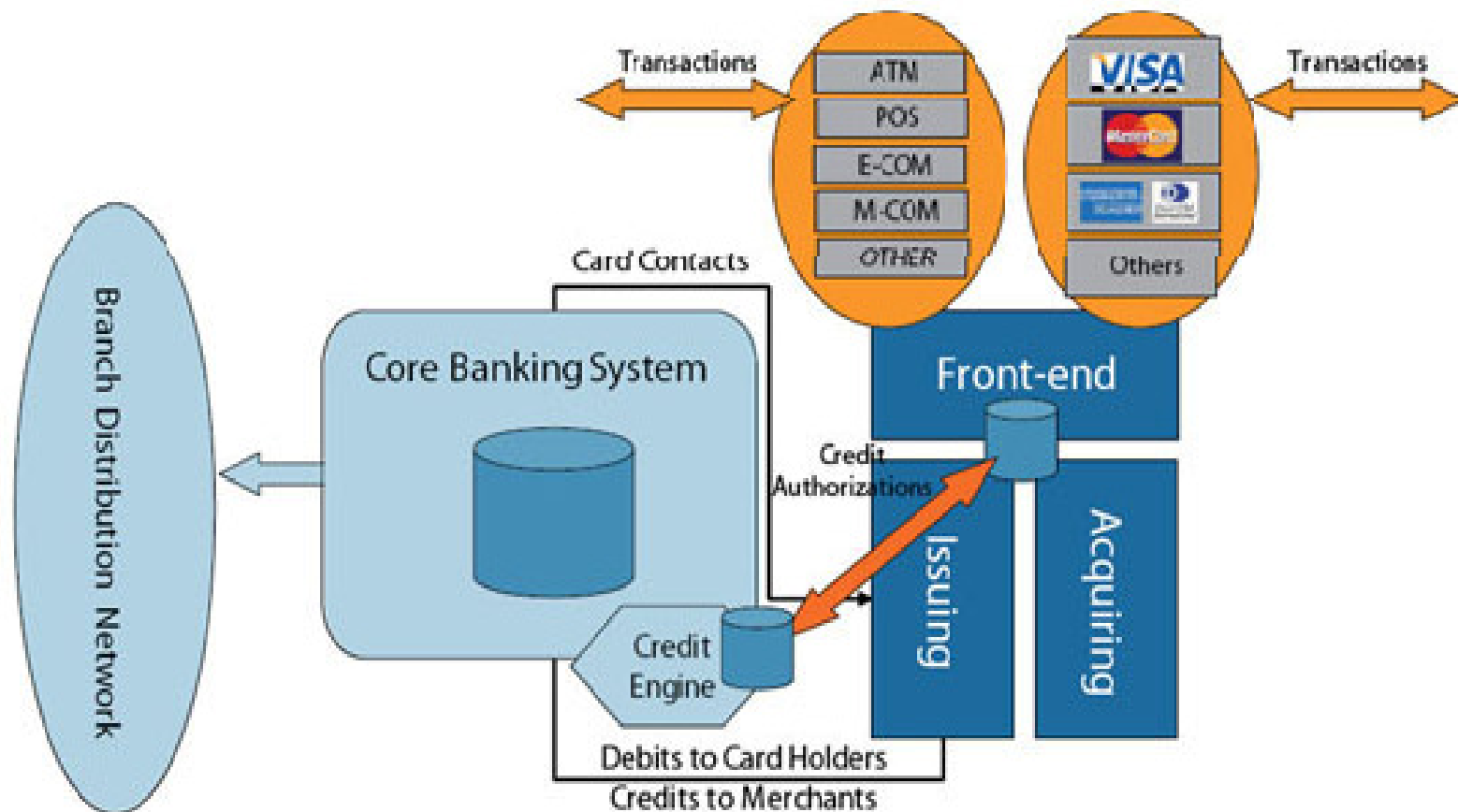


- "CORE" stands for "centralized online real-time environment".
- Core Banking Solution (CBS) is networking of branches, which enables Customers to operate their accounts, and avail banking services from any branch of the Bank on CBS network, regardless of where he maintains his account.

Core Banking Solution

- The customer is no more the customer of a Branch.
- He becomes the Bank's Customer. Thus CBS is a step towards enhancing customer convenience through Anywhere and Anytime Banking.
- In nutshell it means all the bank's branches, Service Outlets (Automated or Manual), Back offices access applications from centralized datacenters.

HOW DOES CBS OPERATE



CORE BANKING SOLUTIONS

- **How shall CBS help Customers?**

All CBS branches are inter-connected with each other by way of software is installed at different branches of bank and then interconnected by means of communication lines.

Therefore, Customers of CBS branches can avail various banking facilities from any other CBS branch located anywhere in the world. All these aim to provide convenient, efficient, and high quality banking experience to the customers, comparable to world class standards.

CORE BANKING SOLUTIONS

The services from CBS are:

- To make enquiries about the balance; debit or credit entries in the account.
- To obtain cash payment out of his account by tendering a cheque.
- To deposit a cheque for credit into his account.
- To deposit cash into the account.
- To deposit cheques / cash into account of some other person who has account in a CBS branch
- To get statement of account.

Core Banking Solution

- To transfer funds from his account to some other account – his own or of third party, provided both accounts are in CBS branches.
- To obtain Demand Drafts or Banker's Cheques from any branch on CBS – amount shall be online debited to his account.
- Customers can continue to use ATMs and other Delivery Channels, which are also interfaced with CBS platform. Similarly, facilities like Bill Payment, I-Bob, M-bob etc. shall also continue to be available. Bank is in the process of launching Internet-banking facility shortly.

Core Banking Solution

- **What are other benefits to the Customers ?**
- A CBS branch is like a Sales & Service Delivery Center. Back office processes/activities are handled through technology at some other site, called Data Center. Branch, therefore, has more time for serving customers.
- This improves the quality and efficiency of the services rendered and the customer is directly benefited by way of satisfying and happy banking experience.

Core Banking Solution

- Since a CBS branch is essentially designed to focus on customer-interface and customer service, the special lay-out and ambience of the branch is made to provide a convenient and delightful banking experience.
- The Customer Service Representatives / Executives at the branch are specially trained to understand, facilitate and deliver banking services efficiently and effectively. We wish our customers happy banking.
- (*To safeguard the interest of customers, Bank has placed certain restrictions on the amount of transactions, which are handled through other branches under CBS. The details can be obtained from the branch).

CBS – SOFTWARES

Types of Banking Softwares With the advent of technology every big bank makes customized software as per its own requirement. These world-class softwares are prepared by reputed software companies in India. These are called core-banking solutions.

Software Name	Developed / Maintained by	Banks in which Implemented
FINACLE	INFOSYS	PNB, OBC, ICICI etc.
FLEX-CUBE	IFLEX	Kotak Mahindra Bank, YES Bank etc.
B@NCS24	TCS	SBI Group
PROFILE	SANCHEZ	ING Vysya Bank
Laser Panacea	Laser Soft	Corporation Bank

BENEFITS OF CBS SOFTWARES

- 1) Reducing operating costs significantly
- 2) Offering improved customer service with higher cross-sell rates with enriched Customer data collection, banks can cross-sell products to existing customers easily.
- 3) Achieving record time-to-market for new products/services from concept to launch.
- 4) Easily integrating with existing systems

BENEFITS OF CBS SOFTWARES

- Helping a bank comply quickly with changing regulatory requirements supports regional regulatory needs (Anti-money-laundering, KYC, Basel II, FEMA, Income Tax Act, etc).
 - (i) Core banking solution is designed on a completely web based paradigm.
 - (ii) It is multi-lingual, multi-currency CRM-enabled core banking solution
 - (iii) Based on open systems and is extensively parameterisable solution
 - (iv) It supports 24x7 operations

Features of CBS SOFTWARES:

- (v) The application has been mostly developed around six basic key foundation concepts.

These are:

- (i) Customer relationship management
- (ii) Modular, parameter-controlled
- (iii) Scalable and high performance
- (iv) System Independence
- (v) Ability to co-exist with other systems through APIs
- (vi) Multilingual and multi-currency

Features of CBS SOFTWARES:

- (vi) It has multiple delivery channel support and the extensibility tool kit. It is fully multichannel alerts-enabled and facilitates bank or customer defined event-triggered alerts to be delivered to the bank's customers through their channel of choice
- (vii) (A) Retail banking Core banking solution supports product management and account management for the full range of retail banking products such as Savings, Current/Checking, Overdraft, Revolving overdraft, Term Deposits and all types of retail Loans [Personal Loans, Auto Loans and Mortgages].

Features of CBS SOFTWARES:

- (B) Corporate banking Provides comprehensive product management and account management for corporate banking products such as Commercial loans, Syndications [Participation], Securitizations, Term Loans, Demand Loans, Overdrafts, Non Performing Asset Management, Limit Management, Debt consolidation through rephasements, Collateral Management, Interest rate management and Loan Modeling.

Features of CBS SOFTWARES:

- (C) Trade finance offers features covering business areas like Bills (Foreign & Inland), Documentary Credits/ Letters of Credit, Pre-shipment Credits, Bank Guarantees, Forward Contracts and Foreign Remittances among others.
- (D) Common modules offers extensive common modules which include support for Clearing (including electronic and RTGS), Standing Instructions, General Ledger, Signature display and management, document tracking, limits and collateral management, delinquency management and a whole range of day to day and year end reports. Finacle has the capability of interfacing with various payment gateways, Anti Money Laundering solutions, Regulatory reporting systems, Statement management and distribution systems and consolidation packages.

Features of CBS SOFTWARES:

- (E) Business benefits provides the bank and its customers a comprehensive unified multichannel view of customers. Its 24x7 availability feature ensures that the bank's customers always stay in touch with the bank. It can help banks eliminate non-productive processes.

Features of CBS SOFTWARES:

- (Viii) Other modules include Accounting (General Ledger) and Executive Information System (EIS) components which leverage the completely integrated nature of the core solution and its automatic data capture characteristics.
- (ix) The solution is being able to accommodate the latest technological innovations through application program interfaces (APIs) which are isolated from the core architecture and do not require the main application code to be re-written.

CONDUCTING THE AUDIT

- **AUDIT METHODOLOGY**



AUDIT METHODOLOGY

- Audit Methodology is the set of procedures to perform the scheduled audit and achieve the audit objectives.
- Audit Methodology also describes the format of the Audit Report and guidelines about completing and gathering the work papers. Work papers include the Templates to test the Internal Controls and evidences collected during the audit.
- Most of the work-papers and/or evidences are in the form of electronic format (Screenshots / diagrams / flowcharts etc.) which should be gathered and preserved to conclude the audit while preparing the final report of the audit.

STEPS FOR AUDIT



AUDIT METHODOLOGY

- Pre-Audit Activities:

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.

AUDIT METHODOLOGY

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.

- 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 :

AUDIT METHODOLOGY

‘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

‘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)** Organizational structure, including reporting lines to the Board of Directors/Senior Management/ Designated Authority.
- **g)** Gradation of IS audit officials/staff

AUDIT METHODOLOGY

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.

AUDIT METHODOLOGY

AUDIT TEAM FINALISATION

- Aligning the audit and technical skill requirements with the skills of the available staff and the development goals of the team members require thought and management skills. The Auditor in Charge (AIC), who will lead the individual audit, must be knowledgeable of the technology, risks and audit techniques unique to the subject and be able to provide guidance and developmental assistance for staff auditors assisting in the fieldwork. The AIC will be responsible for the final product and will approve all the work papers, testing, and results.

AUDIT METHODOLOGY

- The AIC will represent the audit department through the presentation of the final report and ensure that the opinions rendered represent both the risks and controls adequately. Their communication skills (both verbal and written) must be well developed enough to give management the sense that the audit effort is well managed and under control at all times.

AUDIT METHODOLOGY

Communication and Logistics Arrangements

Communication

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.

AUDIT METHODOLOGY

The communication with the auditee 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

AUDIT METHODOLOGY

The Auditor should ensure that Auditee is aware about the other requirements of Auditors like:

- Availability of the respective staff
- Physical Access to the Facility
- Conference Room to be booked for Auditors
- Telephone and Internet Arrangement
- Access to the different IS applications as a GUEST User
- Access to the different IS Applications to use the auditing tool and/or CAATs

AUDIT METHODOLOGY

- Logistics Arrangements
- Information System Auditor should ensure that following logistics arrangements have been made and confirmation about the same should be obtained before travelling.
- Travel Arrangements – Bus/Train/ Flight bookings
- Accommodation Arrangements – Hotel / Guest House
- Pick-up and Drop arrangements to / from accommodation facility to / from office and/or station / airport

AUDIT METHODOLOGY

Data Gathering Sampling

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

- Determining the objectives of the test
- Defining the population to be sampled
- Determining the sampled method i.e. attribute versus variable.
- Calculating the sample size
- Selecting the sample
- Evaluating the sample from audit perspective

AUDIT METHODOLOGY

Risk Assessment

- The steps that can be followed for a risk-based approach to make an audit plan are:
- Take an inventory of the information systems in use in the organization and categorize them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time do they operate.
- Assess what risks affect these systems and the severity of the impact on the business.
- Rank the systems based on the above assessment and decide the audit priority, resources, schedule and frequency.

AUDIT METHODOLOGY

- **Selection of a Risk Methodology**
- In deciding the most appropriate risk assessment methodology, the Information System Auditor should consider the following:
 - The type of information required to be collected (some systems use financial effect as the only measure – this is not always appropriate for Information System Audits)
 - The extent to which the information required is already available
 - The amount of additional information required to be collected before reliable output can be obtained, and the cost of collecting this information (including the time required to be invested in the collection exercise)
 - The opinions of other users of the methodology, and their views of how well it has assisted them in improving the efficiency and / or effectiveness of their audits

AUDIT METHODOLOGY

Use of Risk Assessment

- The nature, extent, and timing of audit procedures
- The areas or business functions to be audited
- The amount of time and resources to be allocated to an audit
- The Information System Auditor should consider each of the following types of risk to determine their overall level:
 - Inherent risk
 - Control risk
 - Detection risk

AUDIT METHODOLOGY

Materiality & Evidence Gathering

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

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

AUDIT METHODOLOGY

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

Evidence:

While evaluating the evidence, Information System Auditors should keep the following points in mind:


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

AUDIT METHODOLOGY

The information System Auditors normally use the following techniques for gathering evidence:

- Reviewing IS Organization Structures
- Reviewing IS Documentation Standards
- Interviewing the Appropriate Personnel.
- Observing the processes and Employees Awareness.

Information System Audit Process

- 
- Opening Meeting
 - Reviewing the documents
 - Interviewing the Key Personnel
 - Conducting Walkthroughs
 - Testing of IS Controls
 - Documentation observations and Findings
 - Audit Report- Preparation & Distribution
 - Audit report
 - Follow Up Activities

Information System Audit Process

Opening Meeting



During the Initial Phase of the audit, this meeting is conducted, to get introduced to the Top Management and Auditee. Audit scope, objective and entire Audit Plan is discussed during the meeting.

Reviewing the documents

An Information system Auditor reviews the following documents to get an overview and understanding about the different processes in the organisation



Information System Audit Process

Following things are to be Reviewed:

- Policies – Are the management guidelines which should be approved by the Top Management and should be reviewed atleast once in each year?
- Procedure – Are the detailed documents based on the policies set by the top management? Procedures contain the detailed information about the process. All the procedure should be approved by the management and should be reviewed atleast once in each year.
- Flowcharts – Pictures are worth thousand words when it comes to understanding the interaction of various processes and how the transaction flow has the dependencies and branches that run in various directions.
- Audit logs and Screenshots – Every organisation implements the monitoring control over the processes and the preserves the evidences of the same, in the form of system screenshots and system logs. This gives an added confidence to the Information System Auditor about the monitoring control established by the management.

Information System Audit Process

Interviewing the Key Personnel



Information System Auditor conducts the meetings and interviews each Dept. / Unit Head as well as with the key personnel working in the operations, to know the following:

- To understand the employee's awareness towards organization's IS policies and procedures.
- Reporting Hierarchy and relationship to understand implementation of SOD (Segregation of Duties) control.
- To gain the knowledge of the entire process and the flow of the data / transactions in the organization.

Information System Audit Process

Testing of IS Controls

Testing of Controls involves the following

- Obtaining the population and conducting the compliance tests either on the entire population and/or on selected samples from the population.
- If any auditing tools are to be used, then the testing is conducted by using the utilities of those tools.

Method of Testing:

- Substantive Testing
- Compliance Testing



Information System Audit Process

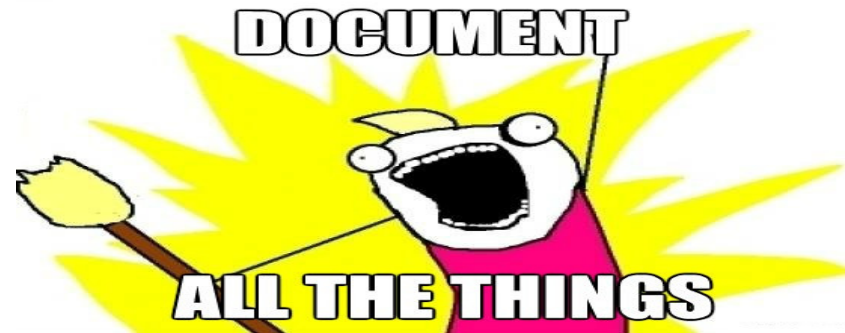
Conducting the walkthroughs

Walkthroughs are conducted to understand the implementation of different processes and gain the evidence for the compliance and/or deviations if any. Walkthroughs include the physical round around the facility, meeting and interacting with the employees, going through the documentations maintained, either Input Forms or Output Forms, by the operations people.



Information System Audit Process

Documenting Observations and Findings



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

- Prove the extent to which an Information System Auditor has complied with guidelines and standards to assist in the planning, performance and review of audits.
- Facilitate third party reviews
- Evaluate the quality assurance program of the Information System Audit function.

Information System Audit Process

- Extend support in circumstances such as insurance claims, fraud cases and lawsuits. Assist in the professional development of the staff.
- Information System Auditors must ensure that at least the minimum level of documentation is maintained as a record of the planning and preparation of the audit scope and objectives.
- Expedite Audit Program
- Audit steps performed and the evidence gathered.
- Audit observations, findings, conclusions and recommendations
- Complete Report issued.
- Facilities Supervisory review

Information System Audit Process

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

- The Information System Auditor's understanding of the area to be audited and its environment.
- The understanding of the information processing systems and the internal control environment
- The author and source of the audit documentation and the date of completion.
- Audit evidence, its source and the date of completion.
- The auditee's response to the recommendations.

AUDIT REPORT

Audit Report – Preparation & Distribution

- Background
- Scope
- Audit Methodology
- Executive Summary
- Conclusion and Roadmap
- Detail Findings
- Observation and/or finding
- Report Distribution -



FOLLOW UP ACTIVITIES

Follow-up Activities

- Usage of Audit Reports
- Reporting of Information System Audit Report
- Follow Up Audit Procedure :
 - Follow up as many steps as possible during the audit
 - Review written responses prior to the review
 - Review only the documentation of corrective action for less critical findings
 - Do not perform audit work at all on minor items
 - Limit follow-up tests to only the problems noted.



Scope of Audit



As per prescribed by the RBI, the General scope of work for IS Audit is as follows:

- *“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”*

SCOPE OF AUDIT

Demo of Scope of Work Related to IS Audit required by various banks:

- I. The Scope of work mainly relates to conducting of Information System and Security Audit of different Information systems in use by the Bank, as listed in Annexure no 1, including those systems used by other agencies for providing services in respect of activities which are outsourced. The IS Audit should be conducted as per the guidelines given by RBI and Govt. of India.

- IS Audit of each of the systems should broadly cover the following aspects:
 - – Physical and Environmental controls
 - – Logical access Controls
 - – Operating System/database review including Vulnerability
 -

SCOPE OF AUDIT

- Assessment
 - – Application Review
 - – Business process Review
 - – Network and Security Review including VA and Penetration test
 - – Backup procedure Review
 - – Business Continuity/Disaster Recovery plans/practices
 - – Review of Outsourced Activities
 - – Virus protection and Patch management.

II. Vulnerability Assessment and Penetration Tests (VAPT) :

The scope also includes conducting Vulnerability Assessment and Penetration Tests (VAPT) covering operating systems, database, networking and Security Infrastructure and various on-line applications facing customers as listed in Annexure 1 and all other assets listed

SCOPE OF AUDIT

III. Application Audit :

The scope further includes Audit of all the Applications used by the Bank. Some critical applications are named here below:

Core Banking Application (E.G– “FINACLE” of Infosys Ltd.) The application and Oracle Database servers are on AIX Unix platform.

Application for Internet Banking

Application developed and being used at our Treasury branch.

Application purchased for our Demat operations.

LAS (Lending Automation Solution)

MIS (Management Information System)

Peoplesoft HRM Solution

MFTP (Matched Fund Transfer Pricing)

SCOPE OF AUDIT

The audit of Applications will be with reference to :

- Auditing Application Architecture with respect to the bank's business/operational requirements, adherence to bank's IT Security Policy, Industry best practices etc.
- Study CBS and other applications for adequacy of Input, Processing and Output controls and conduct various tests to verify existence and effectiveness of controls.
- Review / audit the presence of adequate security features in CBS application to meet the standards of confidentiality, reliability, availability and integrity required for the application supporting business processes.
- Logical access control, User maintenance and password policies being followed are as per bank's IT security policy.

SCOPE OF AUDIT

- Authorisation mechanism and control such as concept of maker checker, exceptions, overriding exceptions and error conditions.
- Controls over automated processing /update of records, review or check of critical calculations such as interest rates, levying of various charges etc., review of the functioning of automated scheduled tasks, batch processes, output reports design, reports distribution, etc.
- Review of all controls including boundary controls, input controls, communication controls, database controls, output controls, interfaces controls from security perspectives.

SCOPE OF AUDIT

- Review effectiveness and efficiency of the Applications. Identify ineffectiveness of the intended controls in the software and analyze the cause for its ineffectiveness. Review adequacy and completeness of controls
- Identify gaps in the application security parameter setup in line with the bank's security policies and leading applicable practices.
- Auditing, both at client side and server side, including sufficiency and accuracy of event logging, SQL prompt command usage, Database level logging etc.
- Complete Review of Application Parameterization.
- Backup/Fallback/Restoration procedures and contingency planning.

SCOPE OF AUDIT

- Review of segregation of roles and responsibilities with respect to application software to improve internal controls.
- Review of documentation for formal naming standards, design process for job roles, activity, groups and profiles, assignment, approval and periodic review of user profiles, assignment and use of super user access
- Manageability with respect to ease of configuration, transaction roll backs, time taken for end of day, day begin operations and recovery procedures
- Special remarks may also be made on following items- Hard coded user-id and password, Interfacing of software with ATM switch, EDI, Web Server and Other interfaces at Network level, Application level Recovery and restart procedures

SCOPE OF AUDIT

- Sufficiency and coverage of UAT test cases, review of UAT defects and tracking mechanism deployed by vendor and resolution including re-testing and acceptance Review of customizations done to the software and the SDLC policy followed for such customization. Proposed change management procedure during conversion, migration of data, version control etc.
- Review of Software benchmark results and load and stress testing of IT infrastructure performed by the Vendors
- Adequacy of Audit trails and meaningful logs
- Adherence to Legal and Statutory Requirements.
- Configuration of System mail

SCOPE OF AUDIT

- Adequacy of hardening of all Servers and review of application of latest patches supplied by various vendors for known vulnerabilities as published by CERT, SANS etc.

- Application-level risks at system and data-level include,
 - system integrity risks relating to the incomplete,
 - inaccurate, untimely or unauthorized processing of data;
 - system-security risks relating to unauthorized access to systems or data;
 - data risks relating to its completeness, integrity, confidentiality and accuracy;
 - system-availability risks relating to the lack of system operational capability;
 - system maintainability risks in terms of adequate change control procedures.

SCOPE OF AUDIT

- As part of documenting the flow of transactions, information gathered should include both computerized and manual aspects of the system.
- Focus should be on data input (electronic or manual), processing, storage and output which are of significance to the audit objective.
- Consideration should be given to audit of application interfaces with other systems or interface of other system with application. The auditor may perform procedures such as a walk-through test.

The scope of work also includes:

- Evaluating completeness of Information System Audit Policy and Information Security Policy of the Bank
- Evaluating completeness of procedures/ guidelines documents
- Evaluating Bank's IT Governance structure including IT Strategy, IT Steering Committee etc.
- Providing minimum baseline security standard / practices in a checklist format to be implemented to achieve a reasonably

SCOPE OF AUDIT

- Secure IT environment for technologies deployed at Bank separately for different Information systems, covering OS, Database, network equipments, security equipments and other relevant aspects of IS Audit.
- Evaluation of Software and Hardware procurement Policy and Maintenance Process.

The scope of work further includes guiding/helping the Bank staff in putting in place the correct practices and conducting of a compliance audit as explained in the Terms of execution of work.

The scope of work also includes extending training to our IS Audit team and to share with them all the formats, check lists, scoring sheets, scripts etc. that will be used during the process of IS Audit. Bank's IS Audit team will be attached to the IS Audit team of the selected vendor, during the course of audit, for obtaining on the job training. The IS Auditor should explain, to the bank's team, all the processes, procedures involved in arriving at audit findings including interpretation of outputs generated by various audit tools. Hands on training for the Bank's team to conduct VAPT and analysis of reports thereof.

SCOPE OF AUDIT

The scope of work includes development of risk profile and drawing up of risk matrix taking into account inherent business risk and effectiveness of the control system for monitoring the risk. Preparation of Risk Matrix should be based upon Risk Analysis of all the Information Systems of the Bank, as per the guidelines issued by RBI and Govt. of India, including following steps :

Step 1: System Characterisation

- Step 2: Threat Identification
- Step 3: Vulnerability Identification
- Step 4: Control Analysis
- Step 5: Likelihood Determination
- Step 6: Impact Analysis
- Step 7: Risk Determination

SCOPE OF AUDIT

The Risk Analysis / Risk Matrix will be based on Adequacy of internal controls, business criticality, regulatory requirements, amount or value of transactions processed, if a key customer information is held, customer facing systems, financial loss potential, number of transactions processed, availability requirements, experience of management and staff, turnover, technical competence, degree of delegation, technical and process complexity, stability of application, age of system, training of users, number of interfaces, availability of documentation, extent of dependence on the IT system, confidentiality requirements, major changes carried out, previous audit observations and senior management oversight.