Controlling & Auditing Information System

Introduction to IT Audit

Prepared by:

Basuki Rahmad, Dr, CISA, CISM

2011

TABLE OF CONTENTS

1 Introduction to IT audit 3
2 Types of IT Audit 3
3 IT Audit Process 5
4 Planning for IT Audit 7
5 Audit Execution 15
6 Reporting and Follow-up 22
7 Quality Assurance 23
8 Use of External Consultants 25
9 IT Audit Standards and Frameworks 33
Annex 1 and 2 36

1 Introduction to IT audit

1.1 Definition of IT Audit

IT Audit can generally be described as the process of obtaining and evaluating evidence to determine whether an IT system safeguards the organisational assets, uses resources efficiently, maintains data security and integrity and fulfils the business objectives effectively.

1.2 Need for IT audit

With the widespread use of computers in even small government organisations for a wide variety of purposes ranging from transaction processing and financial accounting to decision support and data mining systems, it is imperative for auditors to specifically consider the impact of auditee IT systems on their audit methodologies and the techniques of conducting audit tests. While the basic objectives of audit remain the same, it is essential that the personnel entrusted with the task of auditing IT systems acquire sufficient knowledge and skills in understanding and documenting the IT systems, assessing the risks associated with these systems and the adequacy of controls in overcoming / minimising these risks.

1.3 Audit concerns associated with the use of IT systems

As IT is increasingly being used by the auditee organisations to automate their operations, the auditor needs to assess the risks associated with the use of these systems and their vulnerability to these risks. Some of the risks involved in the use of IT systems include among others,

- changes in internal control environment;
- reduced accountability due to anonymity of the users;
- possibility of unauthorised and unrecorded amendments to the data;
- absence of a visible audit trail and/or paper-based documentation;
- changes in audit evidence;
- possibility of duplication / non- inclusion of data;
- new opportunities and mechanisms for fraud and error;
- distributed data storage and processing;
- confidentiality and integrity of key business information;
- increased risks on account of communications within and across organisations, especially the Internet; and
- system failures / shutdowns.

2 Types of IT Audit

IT Audit is a broad term that includes both financial and VFM audit in an IT environment and performance audit of IT systems, depending on the pre-defined audit objective. In the former case, “IT audit” is also called “Auditing in an IT environment” in order to distinguish it from audit of an IT system. However, a common factor is the formation of an opinion regarding the degree of reliance that can be placed on the IT systems in the auditee organization.

Some of the different types of IT audits include the following:

Controls Review	A detailed review of the manual and automated controls in an IT system, with the objective of assessing the extent of reliance that can be placed on the transactions processed and reports generated by the system
Audit of financial systems	Audit of financial statements processed/ generated by an IT system, with a view to expressing an audit opinion
Performance or VFM audit of IT systems	Examination of an IT system to assess whether the intended objectives of implementing the system have been achieved effectively, with due regard to economy and efficiency
Audit of Developing Systems	Concurrent audit of the IT systems development process to assess whether • the system planning, design and development is done in a structured fashion in a controlled environment, and in compliance with the specified methodology; • adequate and effective controls are considered at each stage of the system development process; and • the system provides for an adequate audit trail
Forensic audit	In cases of suspected fraud, illegal acts or violations of company policies and procedures, an investigation to collect audit evidence, by • using appropriate tools/ devices to retrieve data in a legally defensible fashion from computer devices (including PDAs, mobile phones etc.) used by the suspect; and • analyse the data collected to determine the extent of illegal acts and the culpability of persons involved
Security audits	Audits of security controls in IT systems to assess the extent to which confidentiality, integrity and availability of data and systems is maintained, commensurate with the risk profile of the IT system and the organisation
Computer Assisted Audit Techniques (CAATs)	Using automated audit tools and software to: • Download data from auditee IT systems;

	• Analyse auditee data for achieving traditional audit objectives (either financial or performance audit); and • Validation of programs and code in IT systems

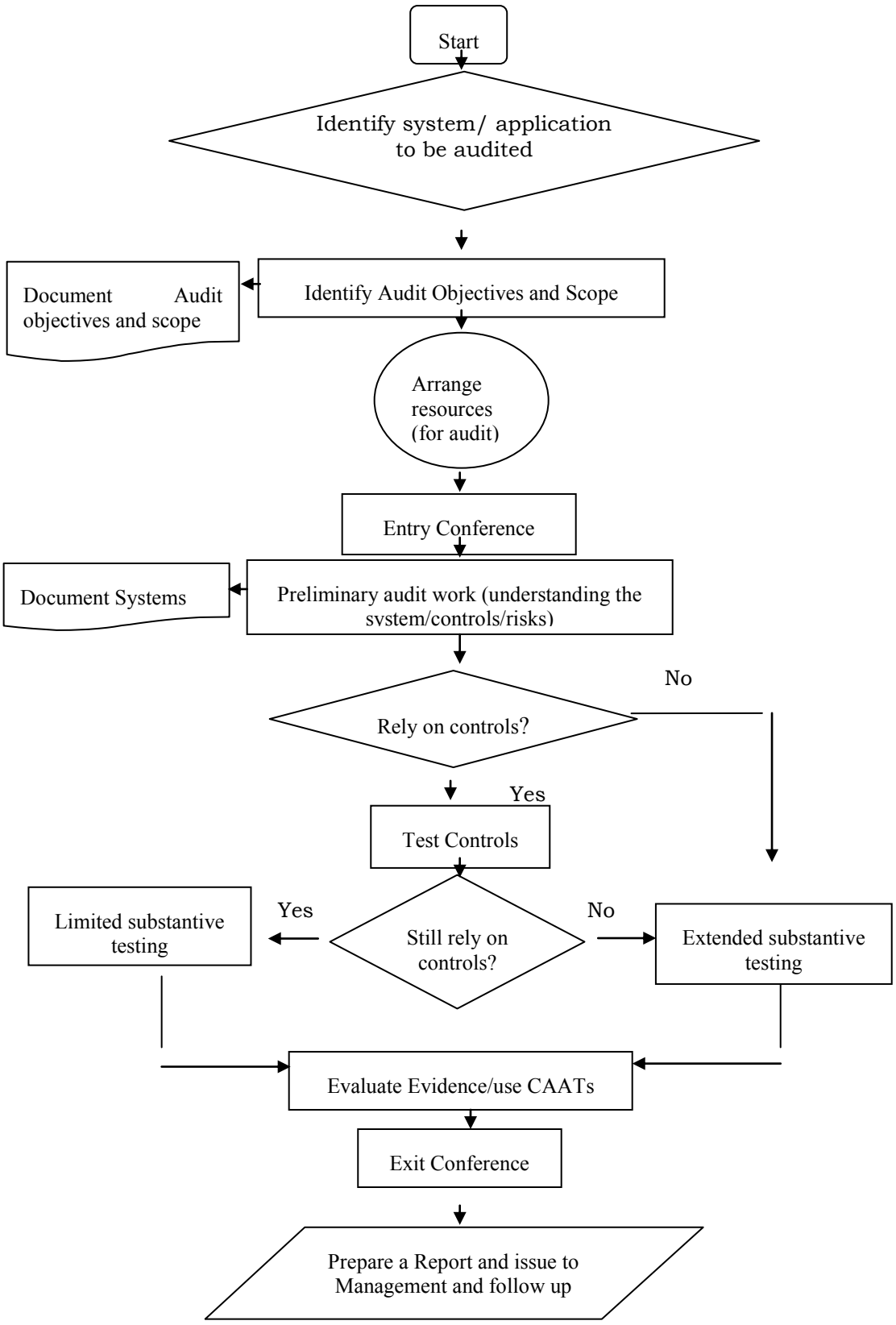
Other uses of IT in an SAI involve automation of supporting functions like audit planning, documentation, management and reporting.

3 IT Audit Process

IT audit process normally involves the following steps:

- Planning
- Evaluation of controls
- Evidence collection and evaluation
- Reporting and follow up

This process is depicted diagrammatically below.


Start
Identify system/ application to be audited
Identify Audit Objectives and Scope
Document Audit objectives and scope
Arrange resources (for audit)
Entry Conference
Preliminary audit work (understanding the system/controls/risks)
Document Systems
Rely on controls?
No
Yes
Test Controls
Still rely on controls?
Yes
No
Limited substantive testing
Extended substantive testing
Evaluate Evidence/use CAATs
Exit Conference
Prepare a Report and issue to Management and follow up

4 Planning for IT Audit

4.1 Overview

Adequate planning is a necessary first step in performing an effective audit of an IT system. Proper planning assists the auditor in:

- the direction and control of his work;
- highlighting critical areas ;
- allocation of scarce audit resources towards more important areas;
- setting time frame and targets for review work ;
- obtaining sufficient, reliable and relevant audit evidence and
- subsequently aid the auditee in sound decision making.

4.2 Strategic plan

This is long term planning, where the targets and objectives for the audit of IT systems of the auditees are determined by the SAI for a period spanning three to five years. This plan should cover all the auditee organisations and address issues like

- aims and long term objectives of audit;
- audit priorities and criteria for prioritisation;
- how to re-orient audit techniques and methods to meet the changing requirements;
- human and infrastructure requirements and
- training needs .

4.2.1 Survey of Auditee IT Systems and Prioritisation

In order to collect information about auditee IT systems (both existing and planned), a detailed survey of auditee IT systems is generally carried out by the SAI, typically once in two to three years. As part of this process, the information detailed in Annex - I is collected.

4.3 Annual plan

This translates the long term plan into a programme of work for the ensuing year. Planning here defines the aims and objectives of each of the major audits to be undertaken during the year, given the resources available within the SAI.

4.4 Micro Plan/ Audit Programme

This is an operational plan for each individual audit and spells out the details of tasks to be undertaken for each audit along with the time schedule. This plan should contain a detailed review of the auditee organisation to determine the extent of assistance, if

any, required from specialist/consultant IT auditors and the division of work between the generalist auditor and the IT auditor. This covers the following aspects:

- Technical Planning
- Logistical Planning
- Risk Assessment

4.4.1 Technical planning

This is the most important aspect of planning an audit - be it performance audit or financial audit, and involves a thorough understanding of the auditee organizations , the business environment in which they operate, their internal control mechanism and the risks involved in the use of IT systems.

As part of this process, the SAI conducts a general review of the IT systems of the auditee to obtain an overview of the

- auditee, the nature of their business and the business environment including their IT strategy and policies, and management and control structures (for both financial and performance audits);
- regulatory environment in which the auditee functions
- details of operating units – number and location
- the size, type, nature and complexity of the IT systems used by the auditee (for financial audit);
- major IT systems , in terms of the value of the systems themselves and their contribution to the achievement of the corporate objectives of the auditee (for performance audit);
- nature of risks the systems are exposed to and the extent of vulnerabilities of the IT systems to such risks;
- critical organizational units/functions
- main types and volume of transactions processed by the systems
- extent and scope of internal audit;

The above details can be gathered by the SAI by,

- touring key organizational facilities
- reading background material including organisation publications, annual reports and independent audit/analytical reports
- reviewing long-term strategic plans
- interviewing key personnel to understand business issues
- reviewing prior audit reports

Gathering this information will enable the SAI to have a sound idea about the type of systems to be audited, indicate priority areas for audit and provide a starting point for audit.

4.4.2 Logistical planning

Logistical planning involves

- allocation of responsibilities of the IT audit team;
- planning the methodology of audit *e.g.* systems based audit (SBA) or direct substantive testing (DST) in the case of a financial audit;
- deciding the scope and extent of audit coverage
- frame the budget (manpower as well as other resource costs), and obtain necessary approvals for resource allocation
- drawing up the time schedule for various tasks;
- exploring ways of obtaining audit evidence and
- framing the reporting requirements.

4.4.3 Resource requirements

The IT auditor must plan the resources required to complete the assigned task. Resources exist in several forms and all must be considered.

4.4.3.1 Staff Resources

The IT auditor may require the skills and services of colleagues or other specialists. When determining needs the IT auditor should bear in mind:

- the level of experience and skills required to perform each task;
- the number of staff required;
- availability of staff. The IT auditor may need to "book" staff early to ensure that they will be available when they are needed; and
- time budgets. Some SAIs may have complex time recording and budgeting systems which are used to control staff resources allocated to each job.

The auditor should also consider what client staff resources are required and their availability.

4.4.3.2 Funds

The IT auditor may need to budget for expenses, especially if the IT review includes an element of travel.

4.4.3.3 Technical resources

The IT auditor may require technical resources to carry out a review. Examples of technical resources include:

- hardware: the IT auditor may require the use of a portable computer to carry out CAATs;
- software : the IT auditor may require audit interrogation software; and
- technical manuals or guidance on the client's systems. e.g. an audit guide on the client's operating system.

4.4.4 Terms of engagement

There are various reasons why an external auditor may be asked to review a client's IT systems. These may include:

- where the external auditor needs to obtain an understanding of the internal controls environment in support of a financial statement audit. In is common for private and public sector auditors to go beyond the minimum necessary to provide an opinion on the financial statements. The auditor may carry out his/her work to provide additional assurance to management and stakeholders (shareholders, public etc) that the systems of internal controls are satisfactory. The auditor may identify control weaknesses and suggest improvements;
- where the auditor has been asked by the client to carry out an IT controls review. The client may wish to know:
    - what controls weaknesses exist, whether they are significant and what can be done about them;
    - how the controls compare to other businesses, i.e. controls benchmarking.
- where the sponsoring government, ministry or department has asked for a review to be carried out on an organisation which is state owned or receives a substantial proportion of its funding from public sector sources;
- where legislation or regulations require regular or periodic controls reviews to be carried out. For example, banks may be required to have annual internal controls reviews carried out on their systems to satisfy national banking laws and finance regulations.

4.4.5 Letters of engagement

In determining the roles and responsibilities of both the client and the auditor, a letter of engagement can be drawn up. Even where an SAI's terms of engagement are set out in legislation, it may be useful to establish, in writing, a clear understanding with the client.

The letter is normally drawn up by the auditor and agreed (signed) by the client. The lead auditor or audit team will normally draft the engagement letter.

For example if the purpose of the audit is to certify the client's financial statements, the lead financial auditor would draft the letter, possibly with input from the IT auditor on IT controls. If the audit was purely an IT controls review the letter of engagement would be drawn up by the IT audit team.

Letters of engagement typically include the client's responsibilities as well as the auditor's responsibilities. For example, a letter of engagement for a financial audit would ensure that the client knows that s(he) is responsible for:

- the proper and complete recording of transactions in the financial statements;
- the safeguarding of the business assets; and
- the accuracy and fairness of the financial statements.

- The letter of engagement may also cover the auditor's responsibilities and what actions will be taken when significant control weaknesses are discovered, e.g. reporting to client management, or regulators.

4.5 Risk Assessment

While prioritising the auditee IT systems for audit, the SAI should carry out a preliminary analysis of the systems to identify the risks that the systems are exposed to, the nature and extent of such risks, the vulnerability of the systems to these risks and the measures that the management has put in place to eliminate/minimise such risks.

Risk management is the responsibility of the top management. It implies the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, considering both the probability and the impact of occurrence. Three security goals of any organization are **C**onfidentiality, **I**ntegrity and **A**vailability. In audit we assess whether any of these goals are infringed upon, and if so, to what extent. Risk assessment is a systematic consideration of

- the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;
- the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and the controls currently implemented.

It is therefore necessary in audit to understand that there is a pay off between the costs and the risks, which are acceptable to the management. For instance, the management might consciously decide that offsite storage is not required in view of low risks, which are acceptable to the business. In other words it is important to study the management perspective and laid down policy before audit comes to a conclusion of acceptable and unacceptable risks.

Therefore, any assessment of the soundness of the IT system will necessarily have to study the policies and process of risk management adopted by an organization. There is need for detailed audit and substantive testing where risk assessment is high and risk management is poor.

It is necessary in the planning stage to study the risk management process of the organization in order to understand the threats as perceived by the management their impact on the systems and to independently assess whether these threats have been countered or guarded against effectively and economically.

An independent risk analysis by the auditor not only helps identify areas that have to be examined but also in determining audit objectives and supporting risk based audit decisions.

4.5.1 Steps in Risk Analysis

The steps that can be followed for a risk-based approach to making an audit plan are:

- Inventory the information systems in use in the organization and categorise them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.

- Assess what risks affect these systems and the severity of impact on the business.
- Based on the above assessment decide the audit priority, resources, schedule and frequency.

Risks that affect a system and should be taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit.

4.5.2 Inherent Risk

Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. For example, the inherent risk associated with application security is ordinarily high since changes to, or even disclosure of, data or programs through application system security weaknesses could result in false management information or competitive disadvantage. By contrast, the inherent risk associated with security for a stand-alone PC, when a proper analysis demonstrates it is not used for business-critical purposes, is ordinarily low.

4.5.3 Controls – An Introduction

Policies, procedures, practices and organizational structures put in place to reduce risks are referred to as internal controls. The extent of internal controls present would determine the risk levels of the application under audit and also the quantum of auditing to be undertaken. In other words, where internal controls are wanting, the extent of audit increases with increased substantive testing and vice versa.

IT controls are grouped as General controls, Application controls and Specific controls. At the planning stage it would suffice for the auditor to form a general opinion on the nature and adequacy of the controls deployed in an IT system and also areas where the Controls are weak and vulnerable. This forms the basis of the extent, the areas, and the depth of testing required. It is also essential that these steps are recorded in detail to serve as pointers.

Internal control activities and supporting processes are either manual or driven by automated computer information resources. Elements of controls that should be considered when evaluating control strength are classified as Preventive, Detective and Corrective with the following characteristics.

Preventive	• Detect problems before they occur • Monitor both operations and inputs • Attempt to predict potential problems before they occur and make adjustments • Prevent an error, omission or malicious act from occurring
Detective	• Use controls that detect and report the occurrence of an error, omission or malicious act
Corrective	• Minimise the impact of a threat • Resolve problems discovered by detective controls • Identify the cause of a problem

	• Correct errors arising from a problem • Modify the processing systems to minimize future occurrence of the problem

4.5.4 Control Risk

Control risk is 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. For example, the control risk associated with manual reviews of computer logs can be high because activities requiring investigation are often easily missed owing to the volume of logged information. The control risk associated with computerised data validation procedures is ordinarily low because the processes are consistently applied.

The preliminary assessment of the adequacy or otherwise of controls could be made on the basis of discussions with the management, a preliminary survey of the application, questionnaires and available documentation. The level of control awareness in the auditee organization and existence or non-existence of control standards are key indicators for preliminary control assessment to be carried out by the auditors. The assessment at this stage also helps fine-tune the audit objectives, which need to be spelt out before commencement of substantive testing.

The auditor should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation. During a review, the auditor will consider the appropriateness of this evaluation in determining the extent to which controls can be relied upon during testing. For example, in using computer programs to test data files, the auditor should evaluate controls over program libraries containing programs being used for audit purposes to determine the extent to which the programs are protected from unauthorized modification. Similarly, if access is not controlled or regulated through say passwords it indicates poor security controls with a high risk of the system getting hacked or breached.

4.5.5 Detection Risk

Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identification of lack of disaster recovery plans is ordinarily low since existence is easily verified.

In determining the level of substantive testing required, the IT auditor should consider both:

- The assessment of inherent risk
- The conclusion reached on control risk following compliance testing

The higher the assessment of inherent and control risk the more audit evidence the IT auditor should normally obtain from the performance of substantive audit procedures.

4.5.6 Identify Control Areas of Risk Management

Based on the assessments of inherent and control risks, including the preliminary evaluation of computer-based controls, the auditor should identify the general control

techniques that appear most likely to be effective and that therefore should be tested to determine if they are in fact operating effectively. By relying on these preliminary assessments to plan audit tests, the auditor can avoid expending resources on testing controls that clearly are not effective.

4.6 Preparation of an audit planning memorandum

The IT auditor should prepare an audit planning memorandum. The purposes of such a memorandum are to:

- define the scope of the IT audit and provide a record of the rationale supporting the decisions relating to the scope and emphasis of the audit, particularly where key decision have been made;
- describe the justification for the audit approach;
- describe how the audit should progress; and
- provide a means for communicating the audit to other assigned audit staff.

4.6.1 Audit Objectives and Scope

Based upon the risk assessment and the control assessment of the application/system selected for audit, the audit objectives are set out. The audit objectives should also take into consideration the managements' objectives for a system. Normally whether the system meets the managements' objectives and serves the business interests in the best possible manner becomes the overall audit objective.

Though it is essential to set out audit objectives clearly for commencement of detailed audit it is necessary to understand that during the course of the audit these objectives could undergo modifications or further elaborations.

As brought out in the definition of IT audit, the broad objectives of IT audit cover an evaluation of the processes to ensure asset safeguarding, the *7S* of data, system effectiveness and efficiency and conformance to rules and regulations. IT audit objectives go hand in hand with any performance, financial or regularity audit objectives that the auditor may set out.

The following is an illustrative list of some of the common audit objectives for an IT audit.

- Review of the controls of the IT systems to gain assurance about their adequacy and effectiveness;
- Evaluation of the main processes involved in the operations of a given area (for instance, the main processes in a billing system would be calculation of bill amount, generation of invoices, collection of dues, tracking delayed payments/non-payments etc) or a system (e.g. payroll system, financial accounting system etc.);
- Evaluation of the performance of a system. For example, billing System or inventory System or a specific programme;
- Review of the security of the IT systems;
- Examine the system development process and the procedures followed at various stages involved therein.

Audit objectives and scope could cover more than just one aspect of the above mentioned areas. For example, review of **system security** could cover merely one of the following aspects or a combination of these:

- Firewall security
- Physical access security
- Passwords
- Security settings
- Account policies
- User rights etc.

Scope defines the boundaries of the audit. Determining the scope of the audit is a part of audit planning. It addresses such aspects as the period and number of locations to be covered and the extent of substantive testing depending on risk levels and control weaknesses. Needless to say the scope of audit will undergo changes as the audit unfolds.

4.6.2 Outline of an audit planning memorandum

An audit planning memorandum would normally contain the following sections:

1. Background of the audited entity:

State : its aims and high level objectives

   - Objectives;
   - Structure;
   - Outline of systems hardware and software;
   - Size of computer operations.

2. State the objectives of the audit:
   - outline the audit approach;
   - outline the scope of the IT auditor's role.
3. Highlight critical areas to be examined : areas where risk is greatest.
4. Resource requirements:
   - Staffing/ Budgets/ scheduling;
   - Technical resources required.

5 Audit Execution

5.1 Entry Conference

A formal audit commencement meeting with the senior management responsible for the area under audit to finalize the scope, understand the special concerns, if any, schedule the dates and explain the methodology for the audit is necessary. This helps fine tune the objectives based on managerial perceptions of the IT system. Such meetings get senior management involved, allow people to meet each other, clarify

issues and underlying business concerns, and help the audit to be conducted smoothly besides apprising the entity of the data, information and documents that will be required by the audit team.

During the entry conference the representatives of the auditee can be apprised of the broad objectives of audit, the proposed tentative audit plan, possible areas of concern based upon previous audit findings or audit findings in similar business areas. Management concerns regarding the IT system are elicited and taken into consideration.

5.2 Evidence Collection and Evaluation

5.2.1 Types of Audit Evidence

When planning the IT audit work, the auditor should take into account the type of the audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. Among the things to be considered are the independence and qualification of the provider of the audit evidence. For example, corroborative audit evidence from an independent third party can sometimes be more reliable than audit evidence from the organization being audited. Physical audit evidence is generally more reliable than the representations of an individual.

The types of audit evidence, which the auditor should consider using, include:

- Observed process and existence of physical items
- Documentary audit evidence (including electronic records)
- Analysis(including IT enabled analysis using CAATs)

5.2.1.1 Physical Evidence

Physical evidence is obtained by observing. It is desirable to corroborate physical evidence, particularly if it is crucial to any audit findings. One of the most desirable corroboration of physical evidence is the acceptance of such evidence by the entity.

Physical verification is the inspection or count by the auditor of a tangible asset. The auditor can physically inspect for the presence of computers, terminals, printers etc. The computer centre should be visited for the visual verification of the presence of water and smoke detectors, fire extinguishers etc. Also, the location of the devices should be clearly marked and visible. Physical access controls are designed to protect the organisation from unauthorised access.

In IT where there is considerable importance given to the physical environment of the systems, audit also has to ensure that the environment conforms to acceptable norms. The aspects verified could range from the location of the fire extinguishers to physical access controls to an inventory of media in an offsite storage location. In such cases observation and corroboration of observed evidence is important.

5.2.1.2 Interview

Auditors can use interviews to obtain both qualitative and quantitative information during evidence collection work. Auditor's use of interviews include the following –

- System analysts and programmers can be interviewed to obtain a better understanding of the functions and controls embedded within the system.

- Clerical/data entry staff can be interviewed to determine how they correct input data that the application system identifies as inaccurate or incomplete.
- Users of an application system can be interviewed to determine their perceptions of how the system has affected the quality of their working life.
- Operations staff can be interviewed to determine whether any application system seem to consume abnormal amounts of resources when they are executed.

Conducting successful interview requires careful preparation. It is necessary to:

- Ensure that the information required is not readily available elsewhere. Alternative sources of the information required might also be found.
- Identify those personnel within an organization who can provide with the best information of an interview topic. Organisation charts often are a first source of information on the appropriate respondents.
- Identify clearly the objectives of the interview and make a list of the information to be sought during the interview. General information should be requested at the beginning and end of interviews. Specific information should be requested toward the middle of interviews. Information requested at the beginning of interviews should be neither controversial nor sensitive.
- Respondents can be contacted to schedule the time and place of their interviews.
- As soon as possible after the termination of interviews, auditors should prepare a report. During the preparation of interview reports, auditors should have two major objectives. First, attempt should be made to separate fact from opinion. Second, auditors should attempt to assimilate the information they obtain during an interview and determine what it means for their overall audit objectives.

5.2.1.3 Questionnaires

Questionnaires have been used traditionally to evaluate controls within systems. Auditors can also use questionnaires to flag areas of system weakness during evidence collection. For example, auditors can use questionnaires to assess users' overall feelings about an information system as an indicator of the system's effectiveness. Similarly, questionnaires can be used to identify areas within an information system where potential inefficiencies exist. Questions must be spelt out clearly, terms must be defined and instructions for completing the questionnaire must be clear. Some general guidelines of questionnaires to be kept in view are to:

- Ensure that questions are specific
- Use language which is commensurate with the understanding of the intended person. For eg. Questions to system administrator or the database administrator need to be specific and may include words which sound like IT jargon but to accurately convey the observation use of these may be inevitable.
- The following need to be avoided unless necessary:
  - ambiguous questions
  - leading questions
  - presumptuous questions

- hypothetical questions
- embarrassing questions

5.2.1.4 Flowcharts

Control flowcharts show that controls exist in a system and where these controls exist in the system. They have three major audit purposes:

- Comprehension – the construction of a control flowchart highlights those areas where auditors lack understanding of either the system itself or the controls in the system;
- Evaluation – experienced auditors can use control flowcharts to recognize patterns that manifest either control strengths or control weakness in a system;
- Communication – auditors can use control flowcharts to communicate their understanding of a system and its associated controls to others.

Constructing a control flowchart involves four steps:

- Choosing the primary flowchart technique that allows particular features of a system to be highlighted and better understood;
- Choosing the appropriate level of detail at which to work so auditors are not overwhelmed with content but nonetheless they do not miss important control strengths or weakness;
- Preparing the primary flowchart so the system features can be easily understood;
- Preparing the control flowchart based on the primary flowchart so control strengths and weakness are manifest.

5.2.1.5 Analytical Procedures

Analytical procedures use comparisons and relationships to determine whether data and account balances appear reasonable. An example is comparing gross margin per cent in current year with the preceding years. Analytical procedures should be performed early in the audit to aid in deciding which accounts do not need further verification, where other evidence can be reduced and which audit areas should be more thoroughly investigated. CAATs can help with the preparation of figures for an analytical review. In particular, CAATs can generate analyses, which would not otherwise be available.

5.2.2 Tools of Evidence Collection

With increased necessity for certification of systems, there is also an increase in the availability of tools which the IT auditors can use. Various kinds of tools are discussed in the succeeding paragraphs.

5.2.2.1 Generalised Audit Software

This is off-the-shelf software that provides the means to gain access to and manipulate data maintained on computer storage media. ACL and IDEA are commonly used examples of generalized audit software. Generalised audit software has been developed specifically to accommodate a wide variety of different hardware and software platforms. They provide a number of functions such as file access, file re-

organisation, selection and extraction of data, various data analysis function and reporting functions. They are used to (a) examine the existence, accuracy, completeness, consistency and timeliness of data (b) the quality of processes embedded within an application system (c) analytical review to monitor key audit indicators such as trend analysis.

Generalized audit software is covered in greater detail in the module on CAATs.

There are limitations to the use of Generalised Audit Software such as limited capability for verifying processing logic and a limited ability to determine propensity for error.

5.2.2.2 Industry Specific Audit Software

Industry specific audit software is designed to provide high level commands that invoke common audit functions needed within a particular industry. To be more specific they provide industry specific logic. For example, financial analysis or ratios geared towards banking industry. Another example is **CAPS** which is specific to the audit of financial institutions and comprises modules such as loan arrears audit, interest audit etc.

5.2.2.3 Specialised Audit Software

This is software written to fulfil a specific set of audit tasks. Most well developed systems have embedded audit modules, which essentially comprise routines that throw up alerts as well as information to ensure continued dependence on controls. Adequacy of the audit module, the data generated by the module, as well as the management's follow up of the audit results are themselves subject to external Government audit scrutiny. To put it simply where the audit module is not operational or has been disabled or is not periodically reviewed there is a higher risk of system violation.

5.2.2.4 Concurrent Auditing Tools

In the manual system of audit, as things stand Concurrent Auditing is not carried out by the external Government auditors. But with increased computerisation there is bound to be an increased dependency on Concurrent Auditing techniques, to collect audit evidence at the same time as an application system undertakes processing of its data. They could be in the form of special audit modules embedded in application systems to collect process and print audit evidence. Most system software comes with embedded audit modules, which help effective supervision by the management.

There are various types of Concurrent Auditing techniques most of which fall into three categories - (a) those that can be used to evaluate application systems with test data while they undertake production processing, (b) those that can be used to select transactions for audit review while application systems undertake production processing, and (c) those that can be used to trace or map the changing states of application systems as they undertake production processing. Some of these techniques are -

- Integrated Test Facility (ITF)
- Systems control audit review file and embedded audit modules (SCARF/EAM)
- Snapshots

- Audit hooks
- Continuous and intermittent simulation (CIS)

5.2.3 Audit Tests

Auditors normally use two types of tests - '**compliance**' tests and '**substantive**' tests.

Compliance tests are concerned with testing the transactions for compliance with rules and regulations of the entity and provide auditors with evidence about presence/absence of internal controls. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary or automated evidence.

Some examples of compliance tests as they relate to the IT environment include:

- Determining whether passwords are changed periodically
- Determining whether system logs are reviewed
- Determining whether program changes are authorised
- Determining whether controls are functioning as prescribed
- Determining whether a disaster recovery plan was tested

Substantive tests provide auditors with evidence about the validity and propriety of the transactions and balances. Auditors use substantive tests to test for monetary errors directly affecting financial statement balances.

Some examples of substantive tests as they relate to the IT environment include:

- Conducting system availability analysis
- Performing system storage media analysis
- Conducting system outage analysis
- Comparing computer inventory as per book vis-à-vis actual count
- Reconciling account balances

Compliance tests determine the extent to which substantive tests may be carried out. Strong controls revealed in the compliance tests can limit the substantive tests and vice versa.

5.2.4 Sampling

Audit efficiency relies on obtaining the minimum audit evidence, sufficient to form the audit opinion. The use of audit sampling, in audit assignments, offers innumerable benefits to auditors. These include:

- providing a framework within which sufficient audit evidence is obtained
- forcing clarification of audit thinking in determining how the audit objectives will be met
- minimising the risk of over-auditing
- facilitating more expeditious review of working papers

- increasing the acceptability of audit conclusions by the auditee as they are seen to be unbiased

Audit sampling is the testing of selected items within a population to obtain and evaluate evidence about some characteristic of that population, in order to form a conclusion concerning the population.

It is important that the items selected should be representative, in order to be able to form a conclusion on the entire population. For example, projecting results of tests applied on only those items having a specific feature, such as high value items only, on the whole population would give skewed results.

There are two primary methods of sampling used by IT auditors,. these are Attribute sampling and Variable sampling. Attribute sampling is generally used in compliance testing situations, and deals with the presence or absence of the attribute and provides conclusions that are expressed in rates of incidence. Variable sampling is generally applied in substantive testing situations, and deals with population characteristics that vary and provides conclusions related to deviations from the norm.

Statistical sampling may be used in different auditing situations. There are different ways in which a statistical sample can be selected. The most frequently used method is random selection where each item in the population has an equal chance of selection. Simple random sampling ensures that every number of the population has an equal chance of selection. It is useful for testing internal controls. For example, the auditor may decide that if there are errors above a certain threshold the control systems are inefficient. The sample could be selected using random numbers through computers. Auditing software such as IDEA could be used for sample selection. Once the sample is selected, identified audit tests are to be applied on the sample.

5.2.5 Evaluation of Evidence

The evaluation process involves weighting and combining the piecemeal evidence collected to make an overall decision. While making the overall decision, auditor must determine whether they believe controls are in place and operating with reliability to ensure the system safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently.

An auditor with his professional skills and knowledge determines as to what should be the status of an existing condition according to the accepted norms. He/she examines the condition as it exists in the live environment and wherever there is significant variation, notes it down as a finding. The findings should have the following characteristics:

- Should be factual and discovered by the auditor;
- Should be based on standards or guidelines against which the conditions are evaluated;
- Effect, impact and significance of the variance should be reported.

In developing the findings, the auditor needs to benchmark the condition. In addition, for the findings to have an impact, the auditor should quantify the significance of the variance in terms of value.

Audit findings have often been regarded as containing the elements of criteria, condition and effect as well as cause when problems are found. However, the

elements needed for a finding depend entirely on the objectives of the audit. This means that the elements 'cause' and 'effect' may be optional for a compliance audit but are a must for an operational audit. Thus, a finding or set of findings is complete to the extent that the audit objectives are satisfied and the report clearly relates those objectives to the finding's elements. A deficiency finding should have five elements or attributes as detailed below.

- Criteria (what should be)
- Condition (what is)
- Cause (why condition occurred)
- Effect (what is the consequence)
- Recommendation (what is to be done)

5.2.6 Significance of Audit Findings

Audit findings need to be significant to be of any use to the audited organization. This is because correcting a deficient audit finding requires resources. The significance can be assessed from two aspects: the nature of the finding itself and the quality of the recommendations. Both quantitative and qualitative aspects of a recommendation should be considered. Examples of quantitative aspects include: revenues increased, cost decreased, number of defects reduced. Examples of qualitative aspects include: citizens/client satisfaction increased, employee morale improved and compliance with laws and regulations is achieved. The goal of system improvement is more likely to be achieved when the recommendations indicate a feasible action plan for the management.

5.3 Exit Conference

After the audit scrutiny is completed, the audit findings and suggestions for corrective action to senior management can be communicated in a formal meeting. This will ensure better understanding and increase buy-in of audit recommendations. It also gives the auditee organisation an opportunity to express their viewpoints on the issues raised. Writing a report after such a meeting where agreements are reached on all audit issues can greatly enhance audit effectiveness. Exit conferences also help in finalizing recommendations which are practical and feasible.

6 Reporting and Follow-up

The report should be complete, accurate, objective, convincing, and as clear and concise as the subject permits. The report should include all significant audit findings. When a finding requires explanation, the auditor should describe the finding, its cause and its risk. When appropriate, the auditor should provide the explanation in a separate reference and make reference to it in the report. This approach may be appropriate for highly confidential matters. IT audit is not effective if audits are performed and reports issued, but no follow-up is conducted to determine if auditee organisation has taken appropriate corrective action. The auditor should have a follow-up program to determine if agreed corrective actions have been implemented. The level of the auditor's follow-up review will depend upon several factors. In some instances, the auditor may merely need to inquire as to the current status. In other

instances, the auditor may have to perform certain audit steps to determine if the corrective action agreed to by the auditee organisation have been implemented.

A typical IT audit would have the following structure:

- Introduction
- Audit Objectives, Scope and Methodology
- Audit Findings
- Audit Conclusions
- Recommendations

7 Quality Assurance

7.1 Supervision and Quality Assurance

Audit records should provide evidence that team leaders have effectively supervised audit projects. Team leaders are also responsible for an appropriate level of technical advice. If particularly complex issues are involved the supervisors should possess, or be able to call on, an appropriate level of knowledge and expertise. Assignment Managers should be actively involved in:

- assignment planning;
- progress control; and
- review.

All audit work requires a combination of compliance with laid down procedures and the exercise of judgement. Review is an internal control which ensures that more than one level of judgement is brought to bear on the work carried out and the conclusions reached. It is concerned with both the quality and the efficiency of the audit and should confirm that:

- the original planned assumptions remain appropriate, taking account of significant events occurring after approval of the audit plan;
- the audit team have properly implemented the audit plan and have performed the audit in accordance with the appropriate Standards;
- the working papers adequately document the work performed by the audit team, particularly in areas where professional judgement has been exercised, and provide the basis for the conclusions expressed in the management letter or report;
- any significant findings have been brought to the attention of the auditee's management, board of directors or audit committee.

7.2 First Stage Review

The Assignment Manager has prime responsibility for compliance with policies and Standards. To ensure compliance, the Assignment Manager should review all working papers in support of the audit and evidence this review. The Assignment Manager may delegate first stage review to a supervisor, but retains overall responsibility.

The reviewer evidences the review by initialling and dating each working paper, although this does not necessarily mean examining each working paper to the same depth. The level of scrutiny depends upon the nature of the area, its materiality, the entity risk and the complexity of audit judgements involved.

The first stage reviewer comments on any matters already identified as warranting attention, and adds any further points that require consideration by the Assignment Director. In each case the reviewer recommends appropriate action. Submission of the matters for attention should not be left until completion of the working papers if the matters for attention are important enough to warrant early involvement of the Director.

7.3 Second Stage Review

The Assignment Director should perform a review of the working papers in sufficient detail to be satisfied that:

- the audit has been conducted in accordance with appropriate Standards;
- the working papers contain sufficient and appropriate evidence to support the management letter or report on the computer information systems, particularly in areas where significant audit judgement has been used;
- the proposed management letter or report is appropriate and supported by the audit evidence.

In addition, the Assignment Director should review all working papers prepared by the Assignment Manager.

The extent of the Assignment Director's review is a matter of judgement and will vary depending upon the experience and knowledge of the audit team, the complexity of the audit and the director's assessment of the risk to the auditors. As a minimum it will normally include:

- the audit plan;
- the summaries of matters for attention and lead schedules on all working paper files;
- ensuring audit programmes have been completed and signed off;
- the evidence supporting all significant audit judgements;
- correspondence with the auditee;
- all original documentation produced by the Assignment Manager.

The Assignment Director evidences the review by initialling and dating all working papers examined. The Assignment Director bases the review on discussion with the Assignment Manager as to how the auditors have responded to key risks identified at the planning stage with the objective of ensuring that sufficient appropriate evidence has been obtained.

7.4 Quality Control Review

A quality control review is carried out after the completion of the audit and presentation of the report or management letter to the auditee. It is conducted by a manager or director who is independent of the audit team. The review focuses on key

areas of professional judgement and compliance with Standards. Reviews are undertaken, often on a sample basis, to ensure that audit work complies with the relevant Standards and that sound judgements have been made.

Each review determines whether:

- the audit has been properly planned and identified risks have received adequate attention;
- conclusions on areas of judgement are explained in and supported by the working papers;
- any other opinion given is fully supported and documented in the working papers;
- the wording of the report or management letter points is appropriate in the circumstances and conforms to relevant Standards;
- the working papers meet the requirements of Auditing Standards in respect of documentation.

In the event of a disagreement between the reviewer and the auditor, both should meet with a higher ranked audit official to resolve the problem to the reviewer's satisfaction. If agreement is not reached then the higher audit official should decide. Once agreement is reached, the working papers are signed off by those responsible for the decision.

The reviewer should be knowledgeable about IT audit and auditing standards. Where specialists have prepared a report it may be appropriate for specialists to review it on a peer review basis.

8 Use of External Consultants

8.1 Introduction

It may be more cost-effective to employ consultants to undertake, or advise on, audits of highly technical and complex elements of Information Systems than to develop in-house the necessary skills which may only be used occasionally.

It may also be cost-effective to:

- market test the entire IT audit service;
- employ consultants to support and develop the unit's IT audit strategy and approach;

Consultants may also be used for specific audit tasks where the necessary skills are not available in the audit body. Skills transfer should be an important objective of such arrangements.

It is important to control the cost of using consultants. The working relationship between auditors and consultants should demonstrate value for money. Contractual arrangements should be established in a manner which allows the audit body to maintain an IT audit approach conforming to appropriate audit standards.

To get the best results from the use of consultants, it is important to:

- identify tasks, opportunities and new approaches where their experience and expertise could benefit the audit;

- select the right consultants for the job (there are a lot of "cowboys" about - look for a proven track record by taking up references);
- bring them in early;
- set firm objectives, clear terms of reference and tight budgets;
- integrate the consultants' contribution with the work of the rest of the team;
- supervise and manage the work through to a successful conclusion; and
- learn lessons for the future.

The following guidance on the selection and use of consultants should help provide a close working relationship that will ensure a successful partnership.

8.2 Why Use Consultants?

The possibility of using consultants, and on what tasks, needs to be considered in the early stages of planning the work. Deciding to bring in consultants after an audit has started is unlikely to be successful. It can take up to three months, and sometimes longer, from identifying the need to issuing the contract.

Always try to alert consultants to possible requirements for their services in good time, both on specific tasks and more generally. They can then plan ahead to help ensure that they are in a position to offer assistance. Too short a period of notice makes it difficult for them to respond to best effect, and to put forward the right staff. Their most appropriate staff resources may be booked up months in advance.

The main reasons for using consultants are:

- to tap into outside experience and expertise and draw on wider disciplines and specialist skills;
- to add breadth and penetration to examinations;
- to identify new approaches and introduce different perspectives;
- to survey best practice in relevant outside fields and activities;
- to provide a cross-check on the auditor's own approach, method and costs;
- to provide extra resources to meet peak workloads;
- to advance delivery dates and help to meet deadlines; and
- to add weight to findings, conclusions and recommendations.

8.3 What Kind of Consultant?

There are no fixed rules on what kind of consultants are best suited to particular tasks or projects. Costs as well as benefits need to be compared in deciding which type of consultancy to choose. The consultant chosen will need to have the resources and ability to meet tight deadlines and possible changes as the work develops.

In practice, the choice is likely to lie within one of three broad categories:

- a consultancy firm or similar organisation;

- an individual or group with an academic or research involvement in the subject or area under examination, or skilled in relevant disciplines or analytical techniques; and
- someone with in-depth experience and an expert practical background in relevant operations or business activities.

Consultancy firms command the largest resources and are able to offer a wider range of services. They have the advantage of being able to draw on a variety of disciplines to provide teams of staff and managers to work in the field as part of the main investigation. It is important to remember that the necessary expertise may be found in the smaller specialist firms as well as the larger management consultancy groups.

Individuals might typically be used to advise on strategic planning and preparatory work as well as on specific examinations. They can be used as part of an audit team, but it is often much easier to use them flexibly - in short concentrated bursts - at successive stages of an examination. Working in this way can be highly cost-effective as well as being attractive to the individuals concerned, since their time is not then tied up for long periods. People who have recently retired from the audited body, or other relevant organisation, should also be considered. They may already be well versed in the audit or operational background to the work.

Both consultancy firms and individuals may be used to review strategic thinking and to suggest ideas for future directions or areas of work. They may advise on plans for individual examinations, and be brought back to review emerging fieldwork results and provide further analysis. They may be used to review final results and the conclusions and recommendations to be included in reports. Their contribution and support are often valuable in the final clearance discussions with auditees.

8.4 Notifying the Auditee

The intention to use consultants on audit examinations should be discussed with the audited body at an early stage. They should also be kept informed as necessary as the work progresses and results emerge.

Although the audited body's views should be fully taken into account, decisions on selection and use of consultants are ultimately the responsibility of the auditor.

Good communications with the audited body gives them the opportunity to:

- put forward any general reservations or suggestions about using consultants;
- confirm their acceptance that the prospective consultants can, in principle, be expected to produce soundly based and authoritative conclusions;
- raise any questions about the access the consultants will need to auditee records, documents and other information, including compliance with Official Secrets Acts or other requirements;
- discuss potential difficulties over individual consultants or consultancy firms, for example on security grounds, on commercial confidentiality or because of possible conflicts of interest with other work; and
- seek information on how the results of the consultants' work will be handled during and at the end of the examination.

8.5 Short-listing Candidates

Having decided on the type of consultancy required, the next step is to identify possible candidates.

Once possible consultants have been identified, further informal enquiries - for example by telephone - should enable a short-list to be drawn up of those available to undertake the assignment and interested in quoting for the work.

These initial discussions are valuable in providing an opportunity for an early assessment of the capabilities of potential bidders. Avoid building up a special or preferential relationship with any individual or consultancy firm competing for the work or otherwise giving them an advantage in securing the assignment. Competitive tenders should be the normal rule.

Make an initial selection from such sources as:

- consultants who have previously carried out successful assignments;
- enquiries amongst known experts in the field;
- professional bodies and similar organisations;
- standard reference sources, for example directories; and
- suggestions by the audited body.

8.6 Financial Control

Likely costs have to be considered at all stages of the work. It is the project manager's job to ensure that sufficient funds are available for the assignment; that costs and commitments are monitored against approved budgets; and that costs are contained and penalties avoided.

However, it is important to remember that costs aren't everything. The quality, speed and timeliness of the work are also crucial factors. Keeping costs under tight control is essential, but it would be foolish to jeopardise the usefulness of the work, and perhaps hinder the investigation as a whole, by taking concern for costs too far.

To ensure sound financial control:

- draw up a specification of the objectives, scope and timing of the assignment;
- prepare a provisional estimate of fees and expenses as soon as possible, and certainly before going out to tender;
- confirm availability of funds and provisional budget approval;
- review the scope of the work and/or budget in light of tenders submitted and confirm revised approval as necessary;
- monitor costs against budget as work proceeds and agree prices in advance for any extra work to be carried out; and
- revise work plans to keep within approved budget, or obtain revised approval as necessary for essential extras.

8.7 Seeking Bids

Bids should normally be obtained by competitive tender. Single tender action may be appropriate where the assignment extends an existing contract won in competition, or where there is clearly only one source of assistance. Exceptionally, this may also be necessary where time is very short. Each auditing body should have established tendering procedures, set out in writing. Consult the appropriate authority for these tendering requirements.

8.8 Assessing Proposals

It is important to decide in advance the criteria to be used to evaluate the individual proposals received from consultants. The main questions to be asked when assessing individual proposals are set out below.

Assessing Consultants' Proposals

- Are the consultants experienced in the field under examination? Are they well versed in public sector concepts?
- Can they demonstrate achievements and results in relevant areas? Have they a good track record?
- Do their proposals conform to the terms of reference? Do they demonstrate a sound grasp of the aims and objectives of the assignment?
- Have they analysed the task requirements carefully and thoroughly? Are their approach and methodology sound?
- Are the individuals who will personally undertake the work capable, experienced and of high quality?
- Is there a clear commitment of partner and senior management back-up?
- Will additional resources be available as necessary to help overcome any problems?
- Are they committed to the timing of the work and meeting the agreed deadlines and delivery dates?
- Do they recognise the importance of clear control and reporting arrangements?
- Are the costs firm and clearly set out? Does the bid provide an appropriate analysis of time and charge-out rates? Are expenses and other costs clearly identified? Are there any "hidden extras"?

8.9 Working Relationships

Good working relationships are essential to get the best out of consultancies. All aspects of an examination should remain under the auditor's control, but it is important to remember that the consultants are an important part of the team and will provide better value for money by being given every opportunity to deploy their experience and abilities.

- Make sure the consultants are kept fully briefed on the objectives of the work as they develop.
- Provide them with the information and co-operation they need to do the job. Keep them up to date with the work of the rest of the team and involve them as necessary in team discussions.
- Brief the consultants on any expected or emerging problems - for example on access to information or sensitivities in relationships - and procedures for resolving them.
- Explain normal arrangements for dealing with the auditee and ensure that the consultants follow them.

- Make it clear that important discussions on findings with the auditee will be led by the auditor. The consultants will, of course, be expected to play a full part in such discussions but should never take over the lead role.
- Watch for any risk of confrontation between specialist consultants and the auditee's own experts.
- Make it clear that the consultants' role as part of the team means that they will operate under the overall management of the team leader.

8.10 Managing the Work

The project manager should make sure that the consultants provide the results expected. This means identifying the crucial elements in the assignment, keeping the consultants informed and monitoring and controlling the various stages of the work. Keeping control of contractors means ensuring that the contract specifies frequent, measurable deliverables and then tracking progress against the agreed schedule. Firm oversight and prompt action are needed.

Working effectively with the consultants means the project manager should:

- set up the necessary liaison arrangements, including timing of interim reports and meetings at key stages;
- make sure from the outset that there is a clear understanding about the scope of the consultants' work, timetable and deadlines;
- encourage two-way traffic and an effective working relationship between the consultants and the rest of the team;
- establish arrangements for identifying and dealing with any emerging problems;
- ensure that any variations to the work, and extra costs, are cleared and approved in advance and the contract amended accordingly; and
- review and discuss the consultants' reports promptly, linking their findings with the work of the rest of the team and ensuring feedback.

8.11 Reviewing Findings

Work done by consultants in effect becomes the work of the auditor. It is not possible to hide behind their reputation or expertise. Therefore, their findings and conclusions need to be independently reviewed to ensure that they meet the required standards.

In specialist fields this may not always be easy, but it cannot be avoided if the final report is to be presented to the auditee and to addressees such as Parliament on a defensible basis.

When reviewing the consultants' work the auditor must:

- be satisfied that the coverage has been carefully planned and that the fieldwork has been properly carried out and is based on sound, documented evidence;
- ensure that the findings and conclusions in the consultants' report are accurate, fair and balanced;
- watch that recommendations are practical and cost-effective;

- check the consistency of their work, findings and recommendations with those of the rest of the audit team;
- pay special attention to those aspects which have caused, or are likely to cause, particular difficulties with the audited body; and
- discuss and resolve potential difficulties with the consultants, and seek their advice on how their work can best be used.

8.12 Consultants' Reports

Careful consideration needs to be given to the best ways of dealing with the consultants' findings when deciding on the content and presentation of the final report to be published. Whichever course is adopted, it should be made quite clear that the audit body stands by the end product and does not distance itself from the consultants' findings.

In some cases, consultants may wish the results of some or all of their work to be published separately, or used for other purposes. This requires the auditing body's approval and cases should be considered on their merits in consultation with the auditee.

Consultants' findings may be used in the following ways:

- no written report by consultants, but findings discussed and incorporated as necessary in final published report;
- consultants submit written report to the auditor, but this is wholly subsumed within the final report;
- consultants' findings are included in whole or in part in final report, and are identified accordingly;
- consultants' report, or summary, is included as a separate chapter or annex in the final report; and
- consultants' report is published separately by the audit body, as complimentary to the main report.

8.13 Assessing Performance and Learning Lessons

It is important to realise the full benefits of the consultancy by learning lessons for the future. This also helps to build up a record of performance as a basis for placing future work. Reviewing the work should be done in frank discussion with the consultant and with the rest of the audit team. The aim should be to learn lessons from successes achieved as well as from any difficulties encountered.

Reviewing the work should be done as quickly as possible, whilst thoughts on both sides are fresh, and a brief written report produced, highlighting good and bad points and assessing the consultants' overall performance.

Main aspects to be covered include:

- Whether the work met the agreed task objectives?
- Whether it was completed within the approved programme and timescale?
- Whether it was delivered within the agreed cost?

- What difficulties arose and why?
- Whether problems were anticipated, or spotted at an early stage, and satisfactorily resolved?
- Whether there was good co-operation and co-ordination with the rest of the audit team?
- Whether the results of the consultants' work were soundly based? Did they make a valuable contribution to the final report?
- Whether the consultants provided other "added value" to the examination?
- What ideas and suggestions do the consultants have for improving future arrangements?
- Whether there are any other lessons for the future?

9 IT Audit Standards and Frameworks

A variety of sources for IT auditing standards and frameworks are available:

- Guidelines, standards and other publications of INTOSAI (in particular, the INTOSAI Standing Committee on IT Audit) and INTOSAI's Regional Working Groups; INTOSAI Auditing Standards do not have mandatory application. They reflect a "best practices" consensus among SAIs. Each SAI must judge the extent to which these standards are compatible with the achievement of its mandate
- the **National** auditing standards body of each country develops its own standards;
- there are auditing standards of the **individual SAIs** and other auditing bodies in each country;
- IS Auditing Standards of the Information Systems Audit and Control Association (ISACA) and the CoBIT Framework of the IT Governance Institute;
- Systems Auditability and Control (SAC) Report and other publications of the Institute of Internal Auditors (IIA);
- standards set by **professional** organisations such as the Information Systems Audit and Control Foundation (ISACF) to which individual auditors may belong as well as
- the international auditing standards promulgated for the private sector by the International Auditing Practices Committee of the International Federation of Accountants (IFAC).
- The "Internal Control – Integrated Framework" and the "Enterprise Risk Management – Integrated Framework" of the Committee of Sponsoring Organisations of the Treadway Commission (COSO)

In addition, with regard to IT security, there are a variety of standards and publications from different sources (which are described in greater detail in the module on IT Security).

Ideally each SAI should have audit standards which encompass IT Audit standards too. In case such standards do not exist, the above standards may serve as frames of reference for the IT auditor to use.

Most of the above mentioned standards, guidance and guidelines are available on the web – some are freely available and others at a price. Brief descriptions of some important frameworks and standards are given in Annex-II.

Annex- I

Illustrative List of Documents Required for Understanding the System.

No.	List of documents
1.	Brief background of the organization
2.	Organizational chart of the entity with details of reporting responsibilities
3.	Personnel policy
4.	Regulations and laws that affect the organisation (for example, Income Tax Act, Company Law etc.)
5.	List of applications and their details
6.	Network and application architecture, including client-server architecture
7.	Organizational structure of the IT department with job descriptions
8.	IT department's responsibilities with reference to the specific application
9.	Business case for the system
10.	Cost associated with the system
11.	Project management reports
12.	Details of hardware
13.	Details of software (including whether developed in-house etc.)
14.	Database details
15.	Data Flow Diagram, Data Dictionary, Table listings
16.	If it is an RDBMS, details of relationships between the tables and database triggers
17.	Details of interfaces with other systems
18.	Systems manual, User manual and Operations manual
19.	Performance analysis reports
20.	List of users with permissions
21.	Input output documents
22.	Test data and test results
23.	Security set up for the system
24.	Previous audit reports

25.	Internal audit reports
26.	User feed back about the system
27.	Peer review reports

Annex – II

Descriptions of some Frameworks/ Standards related to IT Audit

1 ISACA Standards

1.1 General Standards for Information Systems Auditing

The Association's General Standards for IS Auditing apply specifically to IS audits and consist of General Standards covering independence, technical competence, performance of work and reporting:

1.2 ISACA Statements On Information Systems Auditing Standards

The Association issues specific interpretations of the general standards. These are referred to as "Statements On Information Systems Auditing Standards".

1.3 The ISACA Code of Professional Ethics

ISACA Standard No. 3 requires the information systems auditor to adhere to a *Code of Professional Ethics*. This Code of Professional Ethics provides guidance for the professional and personal conduct of members of the Association and holders of the Certified Information Systems Auditor (CISA) designation.

More information on ISACA Standards can be obtained from www.isaca.org.

2 Control Objectives for Information and Related Technology (CoBIT)

COBIT (Control Objectives for Information and Related Technology) is an IT governance framework, which was originally developed in 1994 by the Information Systems Audit and Control Association (ISACA). Version 4.0 of COBIT was released in 2005 by the IT Governance Institute (ITGI). COBIT was designed for three audiences: Management, Users and Auditors. Auditors can make use of COBIT in substantiating their opinion to management on IT internal controls and to be proactive business advisors. COBIT can be extremely useful to the auditors by providing criteria for review and examination, and by providing, through the framework, an approach to improve audit efficiency and effectiveness.

CobiT 4.0 provides good practices across a domain and process framework. Like previous releases of CobiT, CobiT 4.0 leverages the experience of numerous international experts. The CobiT control framework links IT initiatives to the business requirements, organizes IT activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered. CobiT 4.0 represents a consensus of experts from around the world who continually work together to maintain the relevancy, benefit and timelines of CobiT. CobiT 4.0 marks the first major update of the CobiT core content since the release of CobiT 3rd Edition in 2000. The new CobiT volume consists of four sections:

- The executive overview

- The framework
- The core content (control objectives, management guidelines and maturity models)
- Appendices (mappings and crossreferences, additional maturity modelinformation, reference material, a project description and a glossary)

The core content is divided according to the 34 IT processes. Each process is covered in four sections of approximately one page each, combining to give a complete picture of how to control, manage and measure the process. The four sections for each process,in order, are:

1. The high-level control objective for the process
   a) A process description summarizing the process objectives
   b) A high-level control objective represented in a waterfall summarizing process goals, metrics and practices
   c) The mapping of the process to the process domains, information criteria, IT resources and IT governance focus areas
2. The detailed control objectives for the process
3. Management guidelines: the process inputs and outputs, a RACI (Responsible, Accountable, Consulted and/or Informed) chart, goals and metrics
4. The maturity model for the process

Another way of viewing the process performance content is:

- Process inputs are what the process owner needs from others.
- The process description describes what the process owner needs to do.
- The process outputs are what the process owner needs to deliver.
- The goals and metrics show how the process should be measured.
- The RACI chart defines what needs to be delegated and to whom.
- The maturity model shows how the process can be improved.

COBIT, stands for Control Objectives for Information and Related Technology. It was published in 1998 after carrying out revisions in the 2nd edition document by IT Governance institute set up by ISACA

The broad objectives and features are outlined as below:

- COBIT now in third edition helps meet the multiple need of management by bridging the gaps between business risks, control needs and technical issues.
- COBIT is a tool for **IT Governance**. [IT Governance has been defined as a set of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.
- COBIT defines control as "the policies, procedures, practices. and organizational structures designed to provide reasonable assurance that

business objectives will be achieved and that undesired events will be prevented, detected and corrected."

- Within the framework, there are seven business information requirements, or criteria: effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability. COBIT goes on to specify that IT resources provide the information needed by business processes. COBIT framework identifies five types of IT resources: people, application systems, technology, facilities, and data.
- COBIT is a technology independent framework.
- Audience: Management, to help them balance risk and control investment in an often unpredictable IT environment. Users, to obtain assurance on the security and controls of IT services provided by internal or third parties. **Auditors**, to substantiate their opinions and/or provide advice to management on internal controls.
- The framework continues with a set of 34 high level control objectives, one for each of the IT Processes, grouped into four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. The structure covers all aspects of information and the technology that supports it. By addressing these 34 processes' high level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment. Definitions for the four domains identified for the high level classification are:

    i. **Planning and Organizing**: This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realization of the strategic vision need to be planned, communicated and managed for different perspectives. Finally, a proper organization as well as technological infrastructure must be put in place.

    ii. **Acquisition and Implementation**: To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented amd integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

    iii. **Delivery and Support**: This domain is concerned with the actual delivery of required services, which range form traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support processes must be set up. This domain includes the actual processing of data by application systems, often classified under application controls.

    iv. **Monitoring**: All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses managements' oversight of the organization's control process and independent

assurance provided by internal and external audit or obtained from alternative sources.

- **In addition, corresponding to each of the 34 high level control objectives is an Audit guideline to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement. These 318 control objectives were developed from 41 IT Security, audit and control standards and best practice resources, worldwide.**
- In the management guidelines, COBIT specifically provide Maturity Models for control over IT processes, so that management can map where the organization is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organization wants to be; **Critical Success Factors**, which define the most important management oriented implementation guidelines to achieve control over an within its IT processes; **Key Goal Indicators**, which define measures that tell management – after the fact – whether an IT process has achieved its business requirements; and **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

More information on COBIT 4.0 can be obtained from www.itgi.org.

3 IFAC Standards

3.1 Introduction

The International Federation of Accountants (IFAC) is a federation of those national accounting bodies recognised by law or general consensus within their countries as substantial national organisations of good standing within the accountancy profession. It aims to improve the harmonisation of auditing practices throughout the world. Whilst auditors should comply with the national standards of their own country, these should usually match those set by IFAC. Where they differ, auditors should ensure that they comply with the more stringent standard.

The overall objective and scope of an audit do not change with the introduction of a computer information system environment, but the use of a computer will change the processing, storage and communication of financial information and may affect the accounting and internal control systems employed by the entity

3.2 ISA 401 "Auditing in a Computer Information Systems Environment"

This establishes standards and provides guidance on procedures to be followed when an audit is conducted in a computer information system environment. Such an environment exists when a computer of any type or size is involved in the processing

by an entity of financial information of significance to the audit, whether that computer is operated by the entity or by a third party.

ISA 401 sets out considerations for the auditor in determining how a computer information system environment will affect the audit and therefore the audit plan. As the ISA makes clear, a computer information system environment will affect:

- the procedures the auditor will follow in obtaining a sufficient understanding of the accounting and internal control systems;
- the consideration of inherent risk and control risk in determining the risk assessment; and
- the design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

The Standard maintains that a sufficient level of skills and competence must be employed in the audit of a computer information system environment.

3.3 ISA 1008 "Risk Assessments and Internal Control - EDP Characteristics and Considerations. " [Addendum 1 to the ISA on Risk Assessments and Internal Control]

This Standard sets out specific characteristics of a computer information system environment in respect of organisational structure, nature of processing, design and procedural aspects and internal controls (comprising general controls, application controls and control review) to be considered in the assessment of risk in planning an audit.

3.4 ISA 1009 "Computer-assisted Audit Techniques"

This Standard provides guidelines in the use of CAATs, and applies to all uses of CAATs involving a computer of any type or size.

3.5 International Federation of Accountants (IFAC) Statements

Furthermore, three statements have been issued by IFAC which are intended to provide the auditor with guidance in implementing these Standards, but do not have the authority of an ISA. They are:

- Statement 1001, EDP Environments - Stand-alone Microcomputers;
- Statement 1002, EDP Environments - On-line Computer Systems; and
- Statement 1003, EDP Environments - Database Systems.

3.6 IFAC Guidelines

IT Committee of the IFAC came out with a series of guidelines to promote executive understanding of the Key issues affecting the management of information and communications. The series of guidelines were released in the year 2002.

The guidelines are published in six parts – (1) Managing Security of Information, (2) Managing IT – Planning for transact, (3) Acquisition of Information Technology, (4)

The Implementation of IT solutions, (5) IT service delivery and support, (6) IT Monitoring.

In this series of guidelines, the International Federation of Accountants' IT committee seeks to promote executive understanding of key issues affecting the management of information and communications. Everyone including IT auditors who have a specific role and / or responsibility for achieving IT goals and processes can gain from these concepts.

More information on IFAC can be obtained from www.ifac.org.

4 Internal Control-integrated Framework of COSO

The formal name of this report is Internal Control-integrated Framework. It was published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) in September 1992. The official name of the Treadway Commission was the National Commission on Fraudulent Financial Reporting.

As per COSO report, weak internal controls were the primary contributing factor to many fraudulent financial reporting cases. It stressed the importance of the control environment, codes of conduct, audit committee oversight, an active and objective internal audit function, management reports on the effectiveness of internal control and the need to develop a common definition and framework of internal control.

COSO defines internal control as a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

One of the key aspects of this definition is that internal control can provide only reasonable, but not absolute, assurance as to the achievement of the objectives. The report further states that each of the above internal control objectives consists of the following five interrelated components, which are derived from the way management runs a business:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

COSO further states that management is responsible for an entity's internal control system, and the CEO should assume ownership of the control system. As per COSO:

- There is a direct relationship between objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives.
- Internal control is relevant to an entire enterprise, or to any of its units or activities.

- Information is needed for all three categories of objectives to effectively manage business operations, prepare financial statements reliably and determine compliance.
- All five components are applicable and important to achievement of operations objectives.

COSO in its report on Enterprise Risk Management (September 2004) further defined Enterprise Risk Management as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

September 2004 report on Enterprise risk management identified following eight interrelated components of risk management:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and Communication
- Monitoring
- SAC Report of Institute of Internal Auditors.

More information on COSO can be obtained from www.coso.org.

5 Systems Auditability and Control (SAC) Report

The Systems Auditability and Control (SAC) report is intended to provide "sound guidance on control and audit of information systems and technology. The report focuses on the business perspective of information technology and the risks associated with planning, implementing, and using automation." SAC emphasizes management's responsibility to identify, understand, addresses the risks associated with the integration of technology in an organisation, and to oversee and control the organisation's use of technology. The SAC report was originally published by the IIA in 1977. It was the first internal control framework pertaining to IT, Due to the enormous changes in IT since 1977, an updated and extended SAC report was published in 1991, and was then further revised in 1994.

SAC defines the system of internal control as those processes, functions, activities, subsystems, procedures, and organisation of human resources that provide reasonable assurance that the goals and objectives of the organisation are achieved, and which ensure that risk is reduced to an acceptable leve1.

The SAC report consists of fourteen modules: Executive Summary, Audit and Control Environment, Using Information Technology in Auditing, Managing Computer Resources, Managing Information and Developing Systems, Business Systems, End-

User and Departmental Computing, Telecommunications, Security, Contingency Planning, Emerging Technologies, Index, Advanced Technology Supplement, and a case study.

More information on SAC (and the IIA's standards) can be obtained from www.theiia.org.