Manual of Information Technology Audit

Volume I

Office of the Comptroller & Auditor General of India

FOREWORD

It gives me great pleasure to release the Information Technology Audit Manual of Indian Audit and Accounts Department.

Currently India is riding a crest of Information Technology driven growth and the government departments, Public Sector undertakings, Local bodies etc are in no way untouched by this wave. Information technology brings not only changes in the processes but also in the dynamics of working across organizations. The citizens of our country look with great hope towards Information Technology to facilitate transparent governance and speedy development. However since IT systems replace the long standing manual processes it is important to have a certain level of assurance about their working. Along with all their inherent advantages technologies also bring in newer vulnerabilities. This creates an altogether new level of challenges for Auditors which has to be addressed.

Now that IT Audit is a well established function in the department it is imperative that the department has a user friendly manual to guide the Audit parties in conducting quality audits. The present manual fulfils this long standing need of the department. The three volume manual, apart from the theoretical construct, also gives elaborate checklists and audit programmes which can be immediately applied in conducting IT Audits and I congratulate the task force and the IT Audit wing for the effort.

In the field of information technology, more than any other area, the changes are rapid and this manual needs to be kept up-to-date by periodic revisions and supplements in tune with the emerging trends. I am sure that this manual will be a valuable addition to the knowledge and experience of the officers of the department in conducting IT Audits. As more and more IT Audit are conducted in the department it would contribute to the already rich experience in the field and the subsequent additions should be reflective of this process.

(Vijayendra N Kaul)
Comptroller and Auditor General of India

IT Audit Manual

Volume I: The IT Audit process

Table of content

		Page
	Preface	4
SECTION I : THE IT AUDIT PROCESS		
1	Introduction	6
2	Steps in IT Audit	10
3	Preliminary Assessment and Information Gathering	14
4	Risk Assessment to Define Audit Objectives & Scope	17
5	Evidence Collection and Evaluation	23
6	Documentation and Reporting	30
SECTION II : THE IT AUDIT METHODOLOGY		
7	IT Controls	37
8	Audit of General Controls	44
9	Audit of Application Controls	72
10	Audit of IT Security & End User Computing Controls	85
11	Using Computer Assisted Audit Techniques	97
	Annexure: IT Control Frameworks	109
	Glossary	124
	Bibliography	138

Preface

This IT Audit manual is in three volumes. The first volume lays down the IT Audit Process & Methodology in IAAD. The second volume provides practical checklists for the audit party & the third volume provides specific IT Audit Programmes. The Section on IT Audit Process in Volume I also replaces the Chapter 22 on IT Audit of the MSO (Audit) 2002. However some points to be kept in mind are listed below.

Though the manual is wide ranging it cannot be termed comprehensive; maybe no book can lay claim to be so in the rapidly evolving IT environment. Thus one may need to either scope down the checks or supplement them with more advanced material. This would depend upon the level of IT capabilities of the Audit team and the complexity of the application to be audited.

The checklists may be repetitive in a few places. This is due to the fact that good controls tend to be similar in many areas such as IT security, input, processing, output controls etc. However, most of the chapters are so designed that an exhaustive checklist is available for a specific area thus enabling auditors to confine themselves to the defined scope while consulting the manual. Most of the checklists are in the form of questions, but the job of an auditor does not end with getting a Yes/ No answer but starts from there. If the answer is Yes. then it is to be seen to what extent it is true and what are the procedures with associated vulnerabilities. If the answer is No, then it is to be examined why it is so and what is the implication of not having a control in place.

The manual is designed with a high level of granularity but it is important not to miss the wood for the trees. The checklists are intended as aids to the auditor and not to be construed as an end in themselves. They have to be judiciously used depending on the level of complexity and maturity of the systems audited

Suggestions and experiences during IT Audits are invited to be incorporated in subsequent editions.

Deputy Comptroller and Auditor General (LB /AEC)

SECTION I

THE IT AUDIT PROCESS

1. INTRODUCTION

1.1 The advent of Information Technology has changed the way we work in many ways, and audit is no exception. The now almost ubiquitous Computer, though undoubtedly one of the most effective business tools, has also brought with it vulnerabilities of the automated business environment. The pen and paper of manual transactions have made way for the online data entry of computerized applications; the locks and keys of filing cabinets have been replaced by passwords and identification codes that restrict access to electronic files. Each new vulnerability needs to be controlled; assessing the adequacy of each control requires new methods of auditing.

1.2 During the last decade, most of the Government Departments, Public Sector Enterprises and autonomous Bodies have embarked on computerising their operations in a big way. Initially, computers were available only to large organizations due to high purchase and operational costs. Later the advent of personal computers and the rapid decrease in the costs enabled medium-sized organizations also to take advantage of Information Technology for their data processing. Nowadays, the widespread availability of powerful microcomputers and their associated packaged software has resulted in the extensive deployment of computers by even small organizations. Correspondingly the possibilities of data loss and associated organizational costs have increased tremendously along with new risk factors. Due to vulnerabilities of network, the danger of tampering with data by insiders and outsiders is much higher in IS systems.

1.3 Computers themselves have moved from being just electronic data processing (EDP) systems to the realm of Information Technology (IT) Systems since they not only process data but store, utilize and communicate a wide variety of information that influences decision making at various levels of an organization. In fact, with the advent and growth of computer network systems, computer systems are now Information Systems (IS). As a reflection of this evolution, the term “EDP audit” has largely been replaced by such terms as “Information Technology Audit” and “Information Systems Audit”.

1.4 With the increase in the investment and dependence on computerised systems by the auditee, it has become imperative for audit to change the methodology and approach to audit because of the risks to data integrity, abuse, privacy, etc. In an IT system, especially implemented in an environment of deficient controls as compared to a manual system, an independent audit is required to provide assurance that adequate measures have been designed and are operated to minimize the exposure to various risks.

Definition of IT Audit

1.5 The legendary Ron Weber defines IT Audit as *"the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organisational goals to be achieved effectively and uses resources efficiently*".

1.6 IT Audit is a broad term that includes Financial Audits (to assess the correctness of an organization's financial statements), Operational Audits (evaluation of internal control structure), Information Systems Audit(including performance Audit), Specialized Audits (evaluation of services provided by a third party such as outsourcing etc.) and Forensic Audits. 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 audited organization. Audits of Information Technology Systems under development and IT enabled audits (using CAATs) also fall under this broad Grouping.

Objectives of IT Audit

1.7 The objectives of IT audit include assessment and evaluation of processes that

- ✓ (a) Ensures asset safeguarding –'assets' which include the following five types of assets:

- Data

Data objects in their widest sense, i.e., external and internal, structured and non-structured, graphics, sound, system documentation etc.

- Application Systems

Application system is understood to be the sum of manual and programmed procedures.

- Technology

Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.

- Facilities

Resources to house and support information systems, supplies etc.

- People

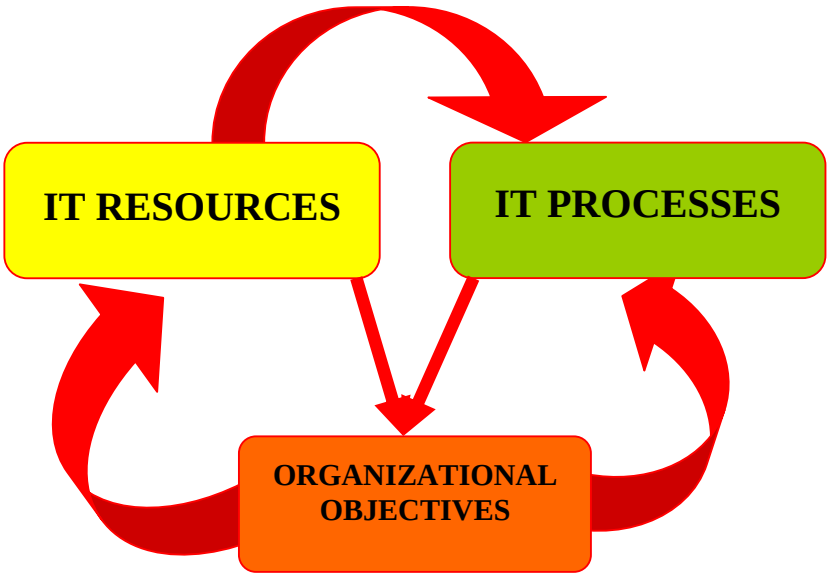
Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

- ✓ (b) Ensures that the following seven attributes of data or information are maintained.

- Effectiveness - deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner. Deals with System effectiveness – evaluating whether the IT system meets the overall objectives of top management and users.

- Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources. Deals with System efficiency – efficient systems use optimum resources to achieve the required objectives
- Confidentiality - concerns protection of sensitive information from unauthorized disclosure.
- Integrity - relates to the accuracy and completeness of information as well as to its validity in accordance with the business' set of values and expectations.
- Availability - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.
- Compliance - deals with complying with those laws, regulations and contractual arrangements to which the business process is subject; i.e., externally imposed business criteria. This essentially means that systems need to operate within the ambit of rules, regulations and/or conditions of the organisation. For example, an FIR to be filed normally requires signature of the complainant as per rules, and needs to be reengineered by changing the rules to permit web based complaints. Similarly, banking operations will have to conform to the banking regulations and legislation. It is also the duty of the IT Auditor to see that the work practices are in tune with the laws of the land such as the IT Act promulgated by the Government of India.
- Reliability of information - relates to systems providing management with appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing information for reporting to the regulatory bodies regarding compliance with laws and regulations.

Thus, IT Audit is all about examining whether the IT processes and IT Resources combine together to fulfill the intended objectives of the organization to ensure Effectiveness, Efficiency and Economy in its operations while complying with the extant rules. This can be depicted diagrammatically as follows:



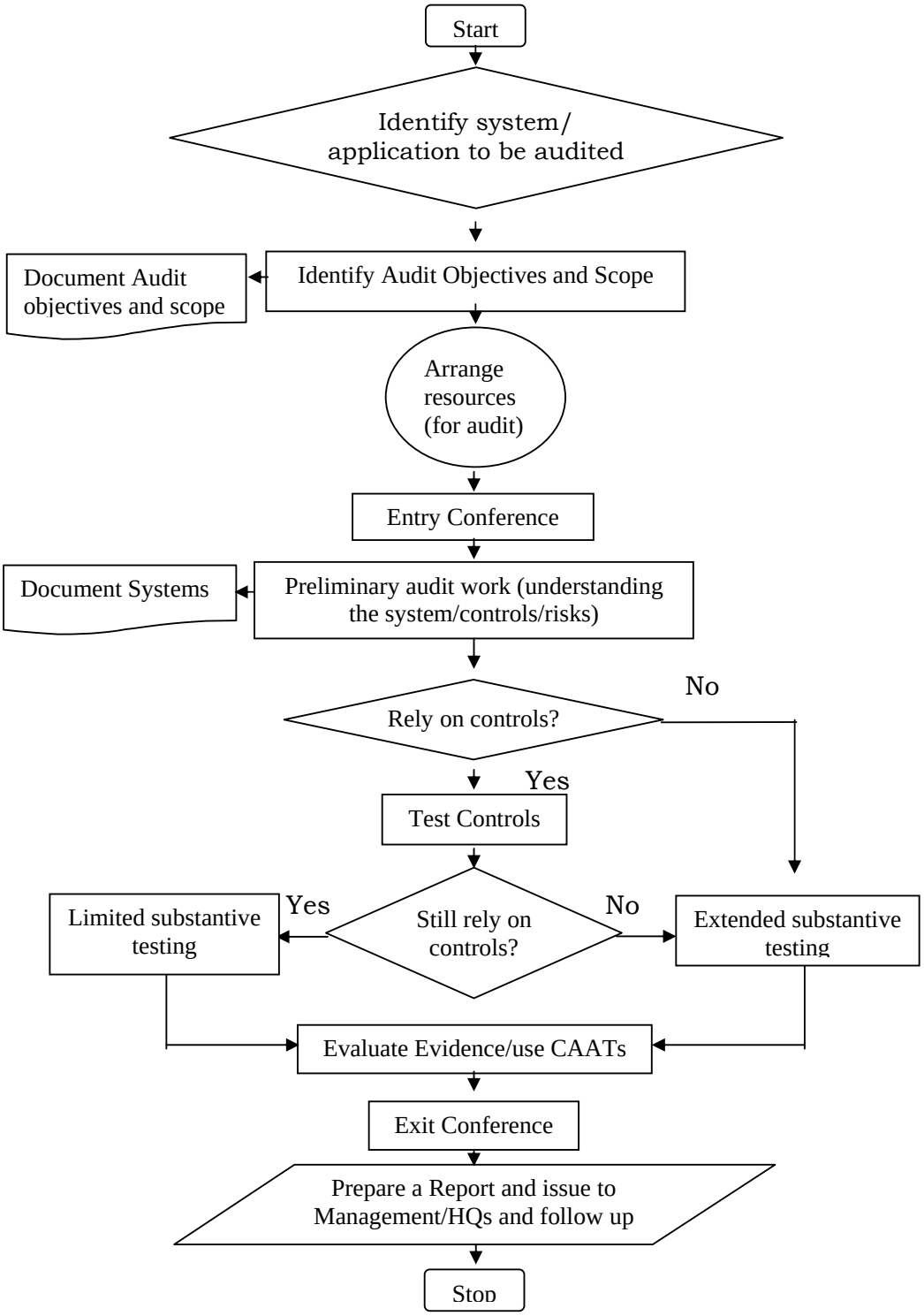
Mandate for IT Audit

1.8 The mandate of SAI India for IT audit is derived from the Constitution of India and established under the Comptroller and Auditor General's (Duties, Powers and Conditions of Service), Act 1971. The mandate of CAG of India for Systems Audit is governed under Sections 13, 14, 16, 17, 18, 19 and 20, as the case may be, read with Section 23 of this Act.

- However of late instances have been noticed where auditees are reluctant to give access to electronic data. This is born more out of a mindset which treats electronic records and manual records as two different entities without realising that it is only the form of the record which is different and not its relevance towards accountability. A certain nervousness is also noticeable in some cases as some of the auditees find it unexpected to have audit looking into their black boxes, the computers.

2. STEPS IN IT AUDIT

IT Audit Process Flow Chart



2.1 The IT audit process has to necessarily include the following steps

- Planning
- Definition of audit objectives and scope
- Evaluation of controls
- Evidence collection
- Evaluation of evidence
- Reporting and follow up

Planning

2.2 The auditing standards of SAI India (paragraphs 4.1, 5.1 and 6.1 under Chapter-III) state that:

- The auditor should plan the audit in a manner, which ensures that an audit of high quality is carried out in an economic, efficient and effective way and in a timely manner.
- The work of the audit staff at each level and audit phase should be properly supervised during the audit; and a senior member of the audit staff should review documented work.
- The auditor, in determining the extent and scope of the audit, should study and evaluate the reliability of internal control.

2.3 Perhaps the most important activity of any audit is planning. The greater the care taken in the planning the more precise and effective will be the audit. Planning is carried out at three levels.

Strategic Plan

2.4 This is long term planning where the targets and objectives for the audit of IT systems of the auditees of the entire IA&AD are determined by the Office of the Comptroller and Auditor General of India for a period of about 3-5 years. This plan should cover all the auditee organizations and address issues like

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

Macro Plan

2.5 This is a medium term plan and translates the long term plan into a programme of work for the ensuing year (the equivalent of our ‘annual audit plan’). Planning here defines the aims and objectives of each of the major audits to be undertaken during the year given the resources available with the field offices.

Micro Plan

2.6 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. The technical and logistical details need to be addressed at this stage.

2.7 The macro and micro plans cannot be static or fixed. They need to be revisited periodically to make adjustments in consonance with the changes in the environment the auditee functions in, as well as changes in risk perception.

IT Audit planning in IAAD

The Comptroller and Auditor General has approved the following procedure for planning, monitoring, processing and approval of IT Audits in IA&AD:

1. Planning of the IT Audits

The selection of topics for IT Audits will be done by the IT Audit wing in consultation with the Field offices and the Functional wings.

2. Monitoring

Pilot studies evaluation, finalization of guidelines, holding workshops, mid term appraisals etc would be done by the IT Audit wing. The concerned functional wings would be kept apprised of the developments.

3. Processing and Approval

After the IT Audit material is received in the IT Audit wing, the IT Audit wing shall process the same through the first journey, second journey and hold discussions with the field offices. The IT Audit material will be examined in the IT Audit Wing with reference to the parameters of IT Audit reporting. In regard to processing and approval of the IT Audit material, the IT Audit wing would clear it from the IT Materiality angle and ensure that the material reaches a stage to be fit for inclusion in the Audit Reports. This would include, as is being currently done, full KD verification (manual and electronic).

i. IT Audit wing may indicate to the functional wing the portions/issues in IT Audit outputs where the functional wing may be requested to take a view or also look into. Conversely, the functional wing may also consult the IT audit wing if the situation demands. In order to avoid breakage of the logical links in the reports, concurrence of the IT Audit wing may be obtained for any

changes made in the report by the functional wings before submitting it to the concerned DAI/ADAI.

ii. *In so far as the audits that are not part of the Annual IT Audit plans and have utilized CAATs for data analysis only, the output would be the responsibility of the functional wings. However, the functional wing may consult the IT Audit wing, if required.*

iii. *Thus IT Audit output would be the joint responsibility of both the IT Audit wing and the respective functional wing. As far as IT materiality is concerned, this shall continue to be the sole responsibility of the IT Audit wing*

4. *Classification of the IT Audits*

The IT Audit reports would be classified into two categories: Transaction Audits and Information Systems Audit. The two would feature in the Transaction Audit reports (Yellow Band) and Performance Audit reports (Blue Band) of the concerned office/functional wing respectively. The Information Systems Audit reports would be clearly identified in a separate chapter labeled as Information Systems Audit. The Information System Audit would encompass amongst other areas like Operational Audits, Information Security Audits, Forensics Audits etc all aspects of Performance Audit relating to the field of IT Audit. The IT Audit wing would suggest classification of the IT Audit material as Information Systems Audit or Transaction audit while forwarding the same to the functional wings.

6. *Dates of submission of the IT Audit reviews*

The schedule of dispatch of the draft IT Audits from the field offices will be synchronized with that of the concerned Report of the respective functional wings so that undue delays are not experienced. The dates of submission of IT Audits would mean the date of submission of the IT Audit paras/reviews to the functional wing by the IT Audit wing for being included in the Bond Copy. However, IT Audit wing shall on receipt of bond copy dates from all the functional wings work out the detailed schedule of submission and intimate to the field offices and the functional wing.

3. PRELIMINARY ASSESSMENT AND INFORMATION GATHERING

3.1 Although concentrated at the beginning of an audit, planning is an iterative process performed throughout the audit. This is because the results of preliminary assessments provide the basis for determining the extent and type of subsequent testing. If auditors obtain evidence that specific control procedures are ineffective, they may find it necessary to reevaluate their earlier conclusions and other planning decisions made based on those conclusions.

Understanding the Organization

3.2 The IT auditor has to perforce gather knowledge and inputs on the following aspects of the entity to be audited:

- Organizational function and the operating environment.
- Organisational structure
- Criticality of systems
- Nature of hardware and software used
- Extent and scope of internal audit
- Nature and extent of Risks affecting the systems

3.3 An understanding of the overall environment can be developed by :

- Reading background material including organisation publications, annual reports and independent audit/analytical reports
- Reviewing prior reports
- Reviewing long-term strategic plans
- Interviewing key personnel to understand business issues
- Visiting key organization facilities

The extent of the knowledge of the organisation and its processes required by the auditor will be determined by the nature of the organisation and the level of detail at which the audit work is being performed. Knowledge of the organisation should include the business, financial and inherent risks facing the organisation. It should also include the extent to which the organisation relies on outsourcing to meet its objectives. The auditor should use this information in identifying potential problems, formulating the objectives and scope of the work, performing the work and considering actions of management for which the IS auditor should be alert.

Organisational Environment

3.4 As part of the planning process, IT auditors should obtain an understanding of the overall environment of the entity. This should include a general understanding of the various business practices and functions relating to the auditee, the types of information systems supporting the activity, as well as the environment it is operating

in. Understanding the organization helps decide what to audit, at what frequency, when, how and to what extent.

3.5 Some essential aspects to be understood about the organisation are as follows:

- The organization's function/business (what it does and how it does it) and its strategic goals and objectives
- The major types, classes and volume of transactions and assets involved in carrying out the business
- The critical organisational units or functions involved in conducting the business
- The number of operating units or locations and their geographic dispersion.
- The key computer based application systems used to process and control these transactions and assets
- Major spending projects or programs in progress or planned for computer systems and equipment
- The types of risks faced by the transactions and assets, computer systems, organizational units, functions, projects and programs involved in the environment within which the business operates and competes
- The regulatory frame work within which the business is carried out

Organisational Structure

3.6 Organizational structure and management controls are an important area of auditor's evaluation to decide upon identification of the line of audit enquiry, determination of audit areas and audit objectives. Organisation and management controls include those controls that provide protection for the actual or tangible physical environment, as well as for the staffing and operation of the information processing facility (IPF). Organisational and management controls within the IPF encompass the following:

- Sound human resource policies and management practices
- Separation of duties between the information processing environment and other organizational environments or functions
- Separation of duties within the information processing environment
- Methods to assess effective and efficient operations

3.7 The IT auditor needs to obtain an understanding of the organisational hierarchy as well as the structure and hierarchy of the IT department. The knowledge of the organisational levels and delineation of the responsibilities provides valuable inputs into supervisory controls and responsibility centres.

Criticality of IT Systems

3.8 IT systems can be categorized as Mission Critical Systems and Support Systems. Mission Critical Systems are those whose failure would have very serious impact on the organisation. Support Systems are those that support management

decision making, the absence of which may not result in as serious an impact as Mission Critical Systems. For example, failure of Air traffic Control System or Railway Reservation System will have serious consequences that may not be the case with failure of a file management system in education department. The scope and extent of audit would be specific to each IT system. Therefore, in planning an audit, the auditor needs to carefully consider the nature of the programmes or functions and the importance to the organisation.

Nature of Hardware and Software Used

3.9 Understanding the hardware details of the organisation in general and IT system in particular is of critical importance to the auditor. This information provides the auditor an understanding of the risks involved. Though the world is moving towards standardized hardware, differences still exist and each type of hardware comes with its own vulnerabilities that require specific controls. The auditor should also evaluate the hardware acquisition and maintenance process as a part of his/her preliminary assessment.

3.10 The auditor needs to understand the type of software used in the organisation. Broadly software can be either developed in house or purchased as a commercial product off the shelf. The policy regarding decision on whether to develop software in-house or buy commercial products needs to be understood. The auditor needs to collect details of operating systems, application systems and Database Management Systems used in the organisation. The auditor as a part of his preliminary information gathering exercise also needs to collect information relating to network architecture used, the technology to establish connectivity, where firewalls are placed etc.

3.11 Preliminary assessment of hardware and software would enable planning the audit approach and the resources required for evidence collection.

4. RISK ASSESSMENT TO DEFINE AUDIT OBJECTIVE AND SCOPE

4.1 Risk management is an essential requirement of modern IT systems where security is important. It can be defined as a process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level, where risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. The 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

Steps in Risk Analysis

4.6 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.

4.7 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.

Inherent Risk

4.8 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.

Control Risk

4.9 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.

4.10 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.

4.11 The Audit Standards of IA&AD (Paragraph 4.7 under Chapter I) state that

"The existence of an adequate system of internal control minimises the risk of errors and irregularities."

4.12 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.

4.13 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.

4.14 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 operation 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

4.15 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.

Identify Controls Areas of Risk Management

4.16 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.

Extent and Scope of Internal Audit

4.17 The internal IT auditor and the external Government IT auditor have complementary roles to play. Where significant amounts of overlap exist, external audit could be suitably modified. The external Government IT auditor has to evaluate the capacity, scope and efficiency of the internal audit function in deciding upon his own checks to be performed to avoid duplication.

4.18 Weak internal audit points to high risk in internal controls and would necessarily result in enhanced external audit. Basic risk areas which the external Government auditor may come across when reviewing internal audit's work include:

Internal audit not reporting to senior management.

Management not required to act on internal audit's recommendations.

Internal Auditor may not be empowered to carry out a full range of assessments or there may be significant restrictions on the scope of its work.

Non-availability of sufficient resources, in terms of finances, staff and skills required

Non involvement of internal audit with IT systems under development.

Detection Risk

4.19 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.

4.20 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.

Risk Assessment Techniques

4.21 There are many risk assessment methodologies available from which the IT auditor may choose. These range from simple classifications of high, medium and low based on the judgement to complex and apparently scientific calculations to provide a numeric risk rating.

Audit Objectives and Scope

4.22 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.

4.23 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.

4.24 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 *IA* 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.

4.25 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.

4.26 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.

4.27 **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.

Logistical Planning

4.28 Logistical planning includes -

- **Manpower planning** – this would cover the identification of the personnel to carry out the audit in specific areas depending upon their expertise and allocation of responsibilities.
- **Methodology of audit –** audit software/hardware to be used, approach to evidence collection, nature of evidence to be collected etc. is identified.
- **Scheduling** - the time schedule for various tasks to be undertaken has to be set out with enough flexibility for mid-stream corrections.

Entry Conference

4.29 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 appraising the entity of the data, information and documents that will be required by the audit team.

4.30 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.

> ☞ In case audit is using CoBIT as the framework for auditing then it may be necessary to make a presentation to the auditee about CoBIT, and if agreed upon then finally a grading can be given for the various domains, objectives etc. These grading would however be applicable only to the report issued to the management, the final report would continue to be drafted keeping in mind the aspect of readability for the general reader.

5. EVIDENCE COLLECTION AND EVALUATION

5.1 Standard 3(e) in chapter-III of the Auditing Standards of SAI India states:

'Competent, relevant and reasonable evidence should be obtained to support the auditor's judgement and conclusions regarding the organisations, programme, activity or function under audit.'

5.2 The standards further prescribe inter-alia that (i) data collection and sampling techniques should be carefully chosen; (ii) the auditors should have a sound understanding of techniques and procedures such as inspection, observation, enquiry and confirmation, to collect audit evidence; and (iii) the evidence should be competent, relevant and reasonable and as direct as possible.

Types of Audit Evidence

5.3 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.

5.4 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)

5.5 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.

5.6 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.

5.7 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.

5.8 The following methods are generally employed for collection of audit evidence:

Interview

5.9 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.

5.10 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.

Questionnaires

5.11 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:

- 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

Flowcharts

5.12 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.

5.13 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.

5.14 **Analytical procedures** use comparisons and relationships to determine whether 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, the CAAT can generate analyses, which would not otherwise be available.

Tools of Evidence Collection

5.15 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.

Generalised Audit Software

5.16 This is off-the-shelf software that provides the means to gain access to and manipulate data maintained on computer storage media. IDEA is a commonly used example 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.

5.17 A detailed note on generalized audit software is available in the Chapter on '**CAATs and Data Downloading'**.

5.18 But, 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.

Industry Specific Audit Software

5.19 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.

Utility Software

5.20 This software performs frequently used functions such as copy, sort, disc search, disc format etc. They often come as part of a suite of programs provided with major system software. Utility software is also available as freeware or shareware or can be purchased and can be used by the auditors either as stand alone or in development of new audit software. Needless to say, the use of Utility software has to be carefully monitored to ensure that permissions and licenses have been obtained.

Expert Systems

5.21 Expert systems are programmes that include knowledge of the expertise developed about a particular domain and use this knowledge to deal with specific problems. Essential to the software is a knowledge base that contains facts about the area of audit and the parameters against which the information being audited is assessed for example norms of emission, which serve as database against which the audited data is compared.

Specialised Audit Software

5.22 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.

Concurrent Auditing Tools

5.23 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.

5.24 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)

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

5.26 **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.

5.27 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

5.28 **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.

5.29 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

5.30 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.

Sampling

5.31 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

5.32 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.

5.33 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.

5.34 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.

5.35 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.

Exit Conference

5.36 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 DOCUMENTATION AND REPORTING

6.1 SAI India's Auditing Standards (Paragraph 8 under Chapter III) state:

'Auditors should adequately document the audit evidence in working papers, including the basis and extent of the planning, work performed and the findings of the audit. Working papers should contain sufficient information to enable an experienced auditor having no previous connection with the audit to ascertain from them the evidence that supports the auditor's significant findings and conclusions.'

Importance of Documentation

6.2 Information systems audit documentation is the record of the audit work performed and the audit evidence supporting audit findings and conclusions. Potential uses of audit documentation include:

- Demonstration of the extent to which the auditor has complied with the Auditing Standards
  - Assistance with planning, performance and review of audits
  - Facilitation of third-party/peer reviews
  - Evaluation of the IT auditing function's quality assurance programme
  - Support in circumstances such as fraud cases and lawsuits

Form, Content and Extent of Audit Documentation

6.3 The auditor should prepare audit documentation that enables an experienced auditor to understand:

- The nature, timing, extent and results of the audit procedures performed
- The audit evidence obtained;
- The conclusions reached on significant matters
- Audit procedures designed to address identified risks of material misstatement,

6.4 Documentation includes a record of:

- The planning and preparation of the audit scope and objectives
- The audit programme
- The evidence collected on the basis of which conclusions are arrived at.
- All work papers including general file pertaining to the organization and system
- Points discussed in interviews clearly stating the topic of discussion, person interviewed, position and designation, time and place.
- Observations as the auditor watched the performance of work. The observations may include the place and time, the reason for observation and the people involved.

- Reports and data obtained from the system directly by the auditor or provided by the audited staff. The IS auditor should ensure that these reports carry the source of the report, the date and time and the conditions covered.
- At various points in the documentation the auditor may add his comments and clarifications on the concerns, doubts and need for additional information. The auditor should come back to these comments later and add remarks and references on how and where these were resolved.
- Where the audit work is reviewed by a peer or a superior, the remarks arising out of the review also should be recorded in the documentation.

The draft and final reports of the audit should form part of the audit documentation.

Identification of Preparer and Reviewer

6.5 In documenting the nature, timing and extent of audit procedures performed, the auditor should record:

- Who performed the audit work and the date of such work; and
- Who reviewed specific audit documentation and the date of such review

Documentation of Specific Items Tested

6.6 In documenting the nature, timing and extent of audit procedures performed, the auditor should record the identifying characteristics of the specific items tested.

6.7 Recording the identifying characteristics serves a number of purposes. For example, it demonstrates the accountability of the audit team for its work and facilitates the investigation of exceptions or inconsistencies. Identifying characteristics will vary with the nature of the audit procedure and the subject matter. For example, a detailed test of entity- generated purchase orders may identify the documents selected for testing by their dates and unique purchase order numbers.

6.8 For a procedure requiring selection or review of all items over a specific amount from a given population, the auditor may record the scope of the procedure and identify the population (for example, all journal entries over Rs.25,000 from the journal register).

6.9 For a procedure requiring inquiries of specific entity personnel, the documentation may include the dates of the inquiries and the names and job designations of the entity personnel.

6.10 For an observation procedure, the documentation may identify the process or subject matter being observed, the relevant individuals and what they were responsible for, and when the observation was carried out.

Audit Evidence

6.11 Electronic evidence is admissible as evidence for consideration of the report at the Headquarters. It should be ensured that as far as possible that timestamps are marked on this evidence invariably. For instance, while making a SQL query, the evidence should include

the query also. In the body of the query, system date and time may also be included, even if for the purpose of the query, this may be irrelevant.

6.12 While using data dumps, to the extent possible, a forwarding letter may be taken. If the same is not possible, the field offices should generate internal documents noting down important information like the date on which the data was handed over, from what file the data dump was created, whether the data was from production environment or from some other environment etc. The electronic evidence generated and used for audit reporting should be related to such documents.

Reply from the Management

6.13 In case of IT Audit Reports, it is extremely important to get the confirmation of /replies to the audit observations. While formal reply may be difficult to get, the concerned field office should try to have meetings with the Management at the highest level and document the findings. Even if these efforts fail, adequate evidence about efforts made should be kept on record and mentioned in the report about these efforts.

Audit Reporting

6.14 It is best to adhere to the normal reporting format for audit reports in case of IT Audit also. The format for audit reviews and audit paragraphs as they are published in the audit reports are well known.

6.15 However wherever CoBIT is used not only as a guideline but as a framework the reporting exercise has to be made as per the structure of the framework. But at the same time the audience for the report should be kept in mind.

6.16 Normally, every field office tends to make every IT Audit report a review. However, in many cases, the materials do not justify a lengthy review. The tendency, therefore, has been to bring in extraneous facts or lose focus in the report. Not all IT audit will result in a lengthy review and in some cases, it should be preferable to propose draft paragraphs focusing on a single issue that audit has come across.

6.17 In the IT Audit, the base of focus in the audit examination is a system. Such a system can run in just one unit or can be spread over a large number of units. For example, a Treasury Accounting System may be spread over many treasuries. A High Tension Billing System, on the other hand, may run in just one branch of an organization. When the system is running in more than one unit, audit examination should be spread over suitably, so that audit conclusions become more representative.

Structure of the Report

6.18 The report should be **timely**, **complete, accurate, objective, convincing**, and as **clear** and **concise** as the subject permits.

6.19 A carefully prepared report may be of little value to decision makers if it arrives too late. The auditors should consider interim reporting, during the audit, of significant matters to appropriate officials. Such communication, which may be oral or written, is not a substitute for a final report, but it does alert officials to matters needing immediate attention and permits them to correct them before the final report is completed.

Report Contents: The report can be broadly structured under the following headings:

Introduction

6.20 A brief introduction to the IT Audit being taken up would be the starting point of the report. The report must briefly give details of the system highlighting application and operating software environment and hardware resources required to run the system. The volume of data, the complexity of processing and other details should also be highlighted so that the reader can gain a clear idea about the system to appreciate subsequent audit findings. The criticality of the system must be assessed and mentioned, as many of the audit observations gain their seriousness from the criticality of the system. If the data flow is complex, a flow chart may be annexed to the report.

Objectives, scope, and methodology

6.21 Knowledge of the objectives of the audit, as well as of the audit scope and methodology for achieving the objectives, is needed by readers to understand the purpose of the audit, judge the merits of the audit work and what is reported, and understand significant limitations.

6.22 In reporting the audit's objectives, auditors should explain the aspects of performance examined. To avoid misunderstanding in cases where the objectives are particularly limited, it may be necessary to state areas that were not audited.

6.23 In reporting the scope of the audit, auditors should describe the depth and coverage of work conducted to accomplish the audit's objectives. Auditors should, as applicable, explain the relationship between the universe and what was audited; identify organizations, geographic locations, hardware and software used and the period covered; report the kinds and sources of evidence; and explain any quality or other problems with the evidence. Auditors should also report significant constraints imposed on the audit approach by data limitations or scope impairments.

6.24 To report the methodology used, auditors should clearly explain the evidence gathering and analysis techniques used. This explanation should identify any significant assumptions made in conducting the audit; describe any comparative techniques applied; describe the criteria used; and when sampling significantly supports auditors' findings, describe the sample design and state why it was chosen.

Audit Results

Findings

6.25 Auditors should report the significant findings developed in response to each audit objective. In reporting the findings, auditors should include sufficient, competent, and relevant information to promote adequate understanding of the matters reported and to provide convincing but fair presentations in proper perspective. Auditors should also report appropriate background information that readers need to understand the findings.

*[**NOTE**: Audit findings not included in the audit report, because of insignificance, should be separately communicated to the auditee, preferably in writing. Such findings, when communicated in a management letter to top management, should be referred to in the audit report. All communications of audit findings should be documented in the working papers.]*

Question of Money value

6.26 The question of money value in IT Audit reporting has been a vexing one. It is acknowledged that in several aspects of IT Audit, especially when the control environment and related issues are being commented upon, any pecuniary loss would be hard to come by. However, when analytical review of data is carried out and the results reported, any sound observation would involve pecuniary aspects. Similarly when aspects like procurement etc. are commented upon, money value will be one of the prime considerations. Thus, a typical IT Audit report in the review format would contain observations with and without money value attached to them.

6.27 Since some of the IT Audit also covers areas like potential risks associated with lack of controls, money value cannot be determined. However, wherever possible, audit should make efforts to approximately calculate the "exposure" when it comments on the risks. This gives a better picture of what is at stake and thus adds credibility to audit observations. The report should also state clearly why such exposure cannot be calculated if audit finds it difficult to do so. For example, if audit is commenting on lack of physical security like fire fighting arrangements, audit should also mention the total value of assets at stake.

6.28 In case of a draft paragraph, normally money value will be one of the most important considerations for processing it further.

6.29 It is also important to remember that importance of money value would have to be seen in the context of the type of application and the organizations role in a larger scheme of things. For example access controls deficiencies in an organization like the defence establishment may not have monetary implications but have serious ramifications. On the other hand in a payroll or an inventory system monetary value would be important unless there is a fraud case, misappropriation, embezzlement etc.

Conclusions

6.30 Auditors should report conclusions as called for by the audit objectives. The strength of the auditors' conclusions depends on the persuasiveness of the evidence supporting the findings and the logic used to formulate the conclusions.

6.31 Sweeping conclusions regarding absence of controls and risks thereon may be avoided, when they are not supported by substantive testing. For e.g. "absence of IT Policy may lead to haphazard IT development in an organization and it may lead to mismatch between hardware procurement and software development" cannot be an audit conclusion even if audit discovers that an organization does not have an IT Policy. Audit should further examine whether it has actually led to haphazard development and whether such development can be ascribed to lack of IT policy and if so, in what way.

6.32 The report should be able to logically link the various observations. For example poor security controls resulting in unauthorized transactions which are found out by using CAATs would more clearly show the overall deficiencies in the IT environment than all these being reported separately.

Recommendations

6.33 Auditors should report recommendations when the potential for significant improvement in operations and performance is substantiated by the reported findings. Recommendations to effect compliance with laws and regulations and improve management controls should also be made when significant instances of noncompliance are noted or significant weaknesses in controls are found. Auditors should also report the status of uncorrected significant findings and recommendations from prior audits that affect the objectives of the current audit.

6.34 Constructive recommendations can encourage improvements. Recommendations are most constructive when they are directed at resolving the cause of identified problems, are action oriented and specific, are addressed to parties that have the authority to act, are feasible, and, to the extent practical, are cost-effective.

6.35 In reporting significant instances of non-compliance, auditors should place their findings in perspective. To give the reader a basis for judging the prevalence and consequences of non-compliance, the instances of non-compliance should be related to the universe or the number of cases examined and quantified in financial terms.

Noteworthy Accomplishments

6.36 Noteworthy management accomplishments identified during the audit, which were within the scope of the audit, can be included in the audit report along with deficiencies. Such information provides a more fair presentation of the situation by providing appropriate balance to the report. In addition, inclusion of such accomplishments may lead to improved performance by other government organizations that read the report.

Limitations

6..37 It is important to mention in the audit report, limitations that were faced by audit. For example, if the data used was not from production environment, it should be so mentioned. Similarly, if there is only production environment and audit could not test dummy data to evaluate input controls comprehensively, it should be mentioned.

6.38 “Read Only Access” given to audit is not a limitation.

☞ No such information about a system should be mentioned in the body of the audit report which might help outsiders to break into the system. Such information, such as table name, path, table structure etc, can only be treated as audit evidence but the reporting has to be carefully monitored. This is particularly true of any network system or a web based ERP systems.

SECTION II

THE IT AUDIT METHODOLOGY

7 IT CONTROLS

7.1 The purpose of the IT Controls module of the IT Audit manual is to provide guidance to IT Auditors for application in the areas of risks, controls, and audit considerations related to Information Systems. It also assists IT Auditors in the scope of issues that generally should be considered in any review of computers related controls over the integrity, confidentiality, and availability of electronic data. It is not an audit standard; however, the IT Controls review work carried out by IA&AD may be influenced by different International Auditing frameworks. These may include INTOSAI Auditing Standards, Control Objectives for Information and Related Technologies (CoBIT) of IT Governance Institute, International Federation of Accountants (IFAC) Auditing Standards, international standards of professional IT audit organisations such as the Information Systems Audit and Control Association (ISACA) and the Institute of Internal Auditors (IIA), etc. IT auditors should familiarise themselves with these standards before taking up an IT audit. The salient features of some of the well known Control assessment frameworks have also been reproduced in Chapter 13.

Definition of IT Controls

7.2 The capabilities of computer systems have advanced rapidly over the past several decades. In many organisations, the entire data has been computerised and all the information is available only in digital media. In this changed scenario, auditors have to adapt their methodology to changed circumstances. While the overall control objectives do not change in a computerised environment, their implementation does. The approach of auditors to evaluate internal controls has to change accordingly.

7.3 *IT Controls in a computer system are all the manual and programmed methods, policies and procedures that ensure the protection of the entity's assets, the accuracy and reliability of its records, and the operational adherence to the management standards.*

7.4 Presence of controls in a computerised system is significant from the audit point of view as these systems may allow duplication of input or processing, conceal or make invisible some of the processes, and in some of the auditee organisations where the computer systems are operated by third party service providers employing their own standards and controls, making these systems vulnerable to remote and unauthorised access.

7.5 When performing IT Control Audit, both types of testing – compliance and substantive testing would be involved. Compliance testing determines if controls are being applied in the manner described in the program documentation or as described by the auditee. In other words, a compliance test determines if controls are being applied in a manner that "complies with" management policies and procedures. Substantive audit "substantiates" the adequacy of existing controls in protecting the organisation from fraudulent activity and encompasses substantiating the reported

results of processing transactions or activities. With the help of CAATs tools, IT auditor can plan for 100 per cent substantive testing of auditee's data.

7.6 Since auditors rely on an assessment of the controls to do their audit, they have to be aware of the impact of computers on the controls. In a computerised environment, there are new causes and sources of error, which bring new risks to the entity. The auditor should consider each of the following factors and assess the overall impact of computer processing on inherent risks. The **impact of the factors** discussed below will typically be pervasive in nature:

- ***Unauthorised access or changes to data or programs***: Applications should be built with various levels of authorisation for transaction submission and approval. Once an application goes into production, programmers should no longer have access to programs and data. If programmers are provided access, all activity should be logged, reported, and reviewed by an independent group. Risks of unauthorised access to data include the possibility of information leaks that would permit outsiders to assess the present state and characteristics of an organisation. Application software and transaction data should be protected from unauthorised alteration by the use of appropriate physical and logical access controls. Physical access controls include the installation of physical barriers to restrict access to the organisation's site, buildings, computer rooms and each piece of IT hardware. Logical access controls are restrictions imposed by the computer software. According to a survey conducted by the Institute of Internal Auditors, forty six percent of the respondents indicated that one of the highest risks in IT systems relate to unauthorised access or changes to data or systems.

- ***Uniform processing of transactions*:** Because computers process groups of identical transactions consistently, any misstatements arising from erroneous computer programming will occur consistently in similar transactions. However, the possibility of random processing errors is reduced substantially in computer-based accounting systems.

- ***Automatic processing*:** The computer system may automatically initiate transactions or perform processing functions. Evidence of these processing steps (and any related controls) may or may not be visible.

- ***Increased potential for undetected misstatements*:** Computers use and store information in electronic form and require less human involvement in processing than manual systems. This increases the potential for individuals to gain unauthorised access to sensitive information and to alter data without visible evidence. Due to the electronic form, changes to computer programs and data are not readily detectible. Also, users may be less likely to challenge the reliability of computer output than manual reports.

- ***Anonymity and reduced accountability*:** The risk of unauthorised transaction processing can be reduced by the presence of controls which positively identify individual users and log actions against them. System owners may reduce the

risks associated with anonymous users by issuing users with unique identifier codes and then forcing authentication of their identity when they log on to the system. Passwords are the most commonly used method of authenticating a user's claimed identity.

- ***Unusual or non-routine transactions*:** As with manual systems, unusual or non-routine transactions increase inherent risk. Programs developed to process such transactions may not be subject to the same procedures as programs developed to process routine transactions. For example, the entity may use a utility program to extract specified information in support of a non-routine management decision.
- ***Concealment or invisibility of some process*:** This weakness can be exploited by embedding unauthorised programs inside authorised ones. The threat of unauthorised program amendments may be reduced by the adoption of appropriate change control procedures, including effective access controls, logging activities, reviewing those logs and an effective separation of duties between system developers, system administrators, computer operations staff and end users.
- ***Inaccurate information*:** Accurate information is an issue whether the end user is accessing a database on the mainframe or a departmental database on a PC. End users may be asked to generate a report without fully understanding the underlying information, or they may not be sufficiently trained in the reporting application to ask the appropriate questions. Additional complications occur when end users download information from the mainframe for analysis and reporting. Departmental databases may have redundant information with different timeframes. The result is wasting time in reconciling two databases to determine which data is accurate. Another major area of concern is that management may fail to use information properly. The reasons for such neglect include:
  - Failure to identify significant information
  - Failure to interpret the meaning and value of the acquired information
  - Failure to communicate information to the responsible manager or chief decision-maker
- ***Existence, completeness, and volume of the audit trail*:** Audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarised. For example, the audit trail for a purchase could include a purchase order; a receiving report; an invoice; an entry in an invoice register (purchases summarised by day, month, and/or account); and general ledger postings from the invoice register. Some computer systems are designed to maintain the audit trail for only a short period, only in an electronic format, or only in summary form. Also, the information generated may be too voluminous to analyze effectively. For example, one transaction may result from the automatic summarisation of information from hundreds of locations. Without

the use of audit or retrieval software, tracing transactions through the processing may be extremely difficult.

- ***Nature of hardware and software used*:** The nature of the hardware and software can affect inherent risk, as illustrated below:
  - The type of computer processing (on-line, batch oriented, or distributed) presents different levels of inherent risk. For example, the inherent risk of unauthorised transactions and data entry errors may be greater for on-line processing than for batch-oriented processing.
  - Peripheral access devices or system interfaces can increase inherent risk. For example, dial-up access to a system increases the system's accessibility to additional persons and therefore increases the risk of unauthorised access to computer resources.
  - Distributed networks enable multiple computer processing units to communicate with each other, increasing the risk of unauthorised access to computer resources and possible data alteration. On the other hand, distributed networks may decrease the risk of data inconsistencies at multiple processing units through the sharing of a common database.
  - Applications software developed in-house may have higher inherent risk than vendor-supplied software that has been thoroughly tested and is in general commercial use. On the other hand, vendor-supplied software new to commercial use may not have been thoroughly tested or undergone client processing to a degree that would encounter all existing flaws.
- ***Weak Security*:** Information systems security should be a concern of both users and management. However, security, for many companies, is not a top priority. In a survey conducted by Ernst & Young and a report by Price Waterhouse, organisations were more concerned with budgets and staff shortages than security. When resources are tight, it is difficult to convince management that spending money for the intangible benefits of security efforts is worthwhile. Respondents to the survey identified obstacles to reducing security risks as a lack of human resources, lack of funds, lack of management awareness, and lack of tools and solutions. However, the survey did discover that organisations have increased their security staff. Advanced technology and increased end-user access to critical information have fuelled the increase in security risks. According to an Info security News survey, the primary concern regarding security involves a lack of end-user awareness.
- ***Unauthorised remote access*:** Some computer operating systems provide for access controls which limit the ability of remote users to see, alter, delete or create data. The operating system's access controls may be augmented by additional identification and authentication controls within each application. In both cases, the effectiveness of access controls is dependent upon strong identification and authentication procedures and good administration of the security systems. More and more users are demanding remote access to Local

Area Network (LAN) services. The easiest way to provide security is to eliminate modem access completely. With weak access controls, a modem allows virtually anyone access to an organisation's resources. To protect against unauthorised access, remote dial up access could have a call-back feature that identifies the user with a specific location. A more-complicated solution is to have key cards with encrypted IDs installed on the remote terminal and a front-end server on the host. At a minimum, user IDs and passwords should be encrypted when transmitted over public lines. In addition, confidential data that is transmitted over public lines should be encrypted. The security solution depends on the sensitivity of the data being transmitted.

- ***Inadequate testing*:** Independent testing is important to identify design flaws that may have been overlooked by the developer of a system. Often, the individuals who create the design will be the only ones testing the program, so they are only confirming that the system performs exactly as they designed it. The end user should develop acceptance criteria that can be used in testing the development effort. Acceptance criteria help to ensure that the end-user's system requirements are validated during testing. For example, the National Institute of Standards and Technology has created a forum of developers and users to exchange testing and acceptance criteria on new IT security products.
- ***Inadequate training*:** Organisations may decide not to invest in training by looking only at the up-front costs. According to one study by the Gartner Group and a recent study by the National Institute of Standards and Technology, the cost of not training far exceeds the investment organisations make to train both end users and IT professionals. One reason for this paradox is that end users who are forced to learn on their own take as much as six times longer to become productive with the software product. Self-training is also inefficient from the standpoint that end users tend to ask their colleagues for help, which results in the loss of more than one individual's time, and they may also be learning inappropriate or inefficient techniques. Both studies also showed that an effective training program reduces support cost by a factor of three to six, because end users who have been trained properly make fewer mistakes and have fewer questions.

Controls in a Computerised Environment

7.7 In a computerised environment, the control components found in manual systems must still exist. However, the use of computers affects the implementation of these components in several ways. Information Technology controls are used to mitigate the risks associated with application systems and the IT environment and broadly classified into two categories. These controls are part of the overall internal control process within any auditee organisation:

- General Controls
- Application controls

General IT Controls

7.8 General controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which the application systems and application controls operate. Examples include IT policies, standards, and guidelines pertaining to IT security and information protection, application software development and change controls, segregation of duties, business continuity planning, IT project management, etc. General IT controls are concerned with the organisation's IT infrastructure, including any IT related policies, procedures and working practices. They are not specific to individual transaction streams or particular accounting packages or financial applications. In most instances the general controls elements of an IT review will concentrate on the organisation's IT department or similar function. Categories of general control include:

Organisation and management controls (IT policies and standards);

IT operational controls;

Physical controls (access and environment);

Logical access controls;

Acquisition and program change controls;

Business continuity and disaster recovery controls.

Application Controls

7.9 Application controls pertain to specific computer applications. They include controls that help to ensure the proper authorisation, completeness, accuracy, and validity of transactions, maintenance, and other types of data input. Examples include system edit checks of the format of entered data to help prevent possible invalid inputs, system enforced transaction controls that prevent users from performing transactions that are not part of their normal duties, and the creation of detailed reports and transaction control totals that can be balanced by various units to the source data to ensure all transactions have been posted completely and accurately.

7.10 Application controls are particular to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance (primarily to management) that all transactions are valid, authorised and recorded.

7.11 Since application controls are closely related to individual transactions, it is easier to see why testing the controls will provide the auditor with audit assurance as to the accuracy of a particular account balance. For example, testing the controls in a payroll application would provide assurance as to the payroll figure in a client's accounts. Many application controls are simply computerised versions of manual controls, e.g. computerised authorisation by a supervisor using an access code rather than putting a signature on a piece of paper.

7.12 As they are related to transaction streams, application controls normally include:

controls over the input of transactions;

controls over processing;

controls over output; and

controls over standing data and master files.

Detailed examination of General and Application Controls is addressed in the succeeding chapters.

8. AUDIT OF GENERAL CONTROLS

8.1 As stated previously, general controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. They create the environment in which IT applications and related controls operate. The IT auditor will focus on general controls that normally pertain to an entity's major computer facilities and systems supporting a number of different IT applications, such as major data processing installations or local area networks. If general controls are weak, they severely diminish the reliability of controls associated with individual IT applications i.e. application controls.

8.2 Following are the major categories of general controls that an auditor should consider:

organisational and management controls;

IT operational controls;

physical controls (access and environment);

logical access controls;

controls for IT acquisition;

program change controls, and

business continuity and disaster recovery controls

8.3 For each of the above categories, this manual identifies critical elements that are basic and essential for ensuring availability of adequate controls. The IT auditor may use the information for evaluating the practices adopted by auditee organisation.

8.4 In order to facilitate the auditor's evaluation, sample audit programs in a tabular format have been summarised in this manual as **the checklists.** These tables can be used for both initial evaluations as well as for documenting the auditor's work regarding testing and audit procedures adopted for IT auditing while carrying out the control assessment work.

Organisational and Management Controls

Control Objective

8.5 These are the high level controls adopted by management to ensure that the computer systems function correctly and that they are satisfying business objectives. The aim of IT auditor will be to determine whether the controls that the auditee organisation has put in place are sufficient to ensure that the IT activities are adequately controlled. In carrying out an assessment, IT auditor should cover the following areas:

- IT planning and senior management involvement
- Personnel and training policies

- Documentation and document retention policies
- Internal audit involvement
- Legal and regulatory compliance
- Segregation of duties

Risk Areas

8.6 An IT auditor should be aware of the following critical elements:

- **Inadequate management involvement may lead to a direction-less IT function** which, in turn does not serve the business needs. This may give rise to problems with the IT systems being unable to meet the business needs;
- **Poor reporting structures leading to inadequate decision making.** This may affect the organisation's ability to deliver its services and may affect its future as a going concern (one of the fundamental accounting principles);
- **Inappropriate or no IT planning leading to business growth being constrained** by a lack of IT resources; e.g. the manager reports to the chief executive that the system is unable to cope with an increase in sales. Overloading a computer system may lead to degradation or unavailability through communication bottle-necks or system crashes;
- **Ineffective staff who do not understand their jobs** (either through inadequate recruitment policies or a lack of staff training or supervision). This increases the risk of staff making mistakes and errors;
- **Disgruntled staff being able to sabotage the system,** for example when staff find out they are going to be disciplined or made redundant;
- **Ineffective internal audit function** which cannot satisfactorily review the computer systems and associated controls;
- **Loss of the audit trail** due to inadequate document retention policies (includes both paper and electronic media); and
- **Security policies not in place** or not enforced, leading to security breaches, data loss, fraud, and errors.

8.7 The organisation and management principles which are relevant to an IT function are the same as those within an organisation's finance function and such high level IT policies, procedure and standards are very important in establishing sound internal controls.

8.8 Management has ultimate responsibility for the safeguarding of the organisation's assets. They are responsible to the stakeholders; taxpayers and citizens in the public sector. Management sets policies to ensure that the risks to the assets are identified and adequately managed.

8.9 Management establishes and approves the policies. The policies are usually high level statements of intent. The policies may feed into standards. Detailed procedures (and controls) flow from the standards. It is important here that while reviewing an organisation's IT policies and standards, the auditor should bear in mind that each auditee organisation is likely to be different and have different organisational

and management requirements. The auditor may assess whether the client's organisational structure and the place of IT within the structure is appropriate.

8.10 **IT Planning and Senior Management Involvement:** one of the major causes for IT project's failures stems out of the little involvement of top management in guiding an IT project. Often IT projects are not perceived to be a part of wider process to deliver business objectives because of very little involvement of top management in defining the required outputs with sufficient clarity and there being no single individual in authority that makes decisions often leading to project failures.

Control objective

8.11 To ensure that in IT Planning and implementation, there exists an active involvement of Senior Level Management so that IT is given the proper recognition, attention or resources it requires to meet business objectives. Also there exists a formal organisational IT structure with all staff knowing their roles and responsibilities, preferably by having written down and agreed job descriptions.

Risk areas

8.12 To have sound and fruitful results from the introduction of IT in the organisation, it is essential to have proper planning and active Senior Level involvement in IT related decisions and their implementation. If such involvement does not exist, there is an increased risk that IT will not be given the recognition, attention or resources it requires, to meet business objectives.

Audit procedure

8.13 The roles and responsibilities of senior management in relation to their business systems should be considered in audit. The auditor should review the high level controls exercised by senior management. An important element in ensuring that projects achieve the desired results is for senior management to take a more proactive involvement during the key project stages:

- Proposal approval;
- Analysis of design and development;
- Selection of product and supplier;
- Implementation and
- Post implementation review.

8.14 Ideally, there should be a steering committee comprised of user representatives from all areas of the business, including the IT department. The Steering Committee would be responsible for the overall direction of IT. The nature of the IT Steering Committee will vary according to the client's circumstances. For example, a large government department would be expected to have a formal IT Steering Committee, whilst in a small organisation, the IT Steering Committee may be small and informal. The IT Steering Committee would be responsible for issues beyond just the accounting and financial systems, for example, the telecommunications system (phone lines, video-conferencing), office automation, manufacturing processing systems etc. To be effective, the IT Steering Committee should draw its members from senior and

middle management. Membership should be drawn from all user departments within an organisation. Senior management's place is especially important since their presence gives the decisions made by the committee greater weight and also ensures that IT is business driven and not technology driven.

8.15 Once the Steering Committee agrees on a future direction for IT, the decisions should be formalised and documented in a plan. The future direction agreed by the IT Steering Committee is normally set out in a document known as the IT strategic plan. The IT strategic plan is in effect the starting point for any investment in IT as it identifies future changes which have to be budgeted for. The decisions and planned changes specified within the IT long term plan would then feed into the IT department's tactical plans.

8.16 An IT strategic plan to be endorsed by top management is very important from the following considerations:

- Effective management of information technology is a business imperative and increasingly a source of competitive advantage. The rapid pace of technological changes together with the declining unit costs, are providing organisations with increasing potential for:
  - Enhancing the value of existing products or services;
  - Providing new products and services; and
  - Introducing alternative delivery mechanisms.
- To benefit from information technology requires foresight to prepare for the changes, planning to provide an economical and effective approach, as well as, effort and commitment in making it happen.
- Information technology planning provides a structured means of addressing the impact of technologies, including emerging technologies, on an organisation. Through the planning process, relevant technologies are identified and evaluated in the context of broader business goals and targets. Based on a comparative assessment of relevant technologies, the direction for the organisation can be established.
  - The implementation of information technologies may be a complex, time consuming and expensive process for organisations. Information technology planning provides a framework to approach and schedule, information technology projects in an integrated manner wherever possible. Through this process, performance milestones can be agreed upon, scope of specific projects established, resources mobilised and constraints or limitations identified. Without effective planning, the implementation of information technologies may be misguided, haphazard, delayed and more expensive than justified.
  - Good governance requires that all investments be justified — including any information technology investments. Information technology planning provides a process for not only evaluating alternative approaches, but also

for justifying the selected approach in terms of benefits, both tangible and intangible, that will be realised by an organisation. This is an important dimension when many of the underlying projects may be difficult to support on an individual basis.

8.17 Although the IT strategic plan is likely to have a minimal effect on the current year's audit it may have a significant effect on future years' audits. A review of an organisation's IT strategic plan could forewarn the IT auditor of problems which may arise in later years. For example, the IT plan may state that the organisation will replace its financial system in two years time. This may have an impact on the work of the auditor.

8.18 The organisation should develop information technology plans which reflect its corporate strategy and match its information technology needs for a given future period. Notwithstanding the uniqueness of a business perspective, an information technology plan must be based on the following:

- It should support and complement the business direction of an organisation.
- The scope of the plan should be established to facilitate formulation of effective strategies.
- A planning horizon should be formulated that provides long-term direction and short-to-medium term deliverables in a manner consistent with the business strategy.
- Costs of implementation should be justified through tangible and intangible benefits that can be realised.
- The planning process should recognize the capability and capacity of the organisation to deliver solutions within the stated planning timeframe.
- It should provide a basis for measuring and monitoring performance.
- It should be reassessed periodically.
- It should be disseminated widely.
- Responsibility for implementing the plan should be explicit.
- Management commitment in implementing the plan should be exhibited.

8.19 **Controls Over IT Acquisition**: the importance of IT related acquisitions is usually directly proportional to their post, scale and complexity. In general, the larger and more complex the acquisition, the higher will be its impact on, and importance to, the business. In addition, the acquisition may be important to the business due to its interrelationships with other IT projects.

Control Objective

8.20 A structured acquisition process provides a framework for ensuring that:

- there are no major omissions from a business, technical or legal standpoint;
- the costs and resources for the acquisition process are appropriate and are efficiently deployed;
- the validity of the business case in support of the acquisition is reaffirmed prior to selecting a solution; and

- there is progressive buy-in to the new system as a result of user group involvement throughout the acquisition process.

Risk Areas

8.21 Critical elements involved in the process of acquisition of IT assets are as follows:

- In IT systems, the scale, cost and impact of an acquisition may have a strategic significance well beyond the acquisition itself. Any serious misjudgement in the acquisition decision will impair not only the success of the underlying IT project but, in addition, the potential business benefits that are anticipated.
- Acquisitions frequently involve a significant capital investment for an organisation. In addition to the investment, the opportunity cost of the capital employed and the time/resources expended in the acquisition process add to the importance of the acquisition.

Audit Procedure

8.22 As a prudent IT auditor, it must be seen that the process adopted for acquisition of IT Assets should encompass the following elements:

- adherence to a structured approach, comprising all the key acquisition activities and deliverables, timelines and milestones, project organisation and resources;
- enunciation of objectives, including a concise statement of the business expectations from the acquisition, detailed requirements, and specification of overall scope;
- defined evaluation and selection criteria, particularly measurement scale, relative weights of all criteria and the manner in which acquisition and project risks will be minimised;
- commitment and support of executive management through a senior level project sponsor and, if appropriate, the establishment of an acquisition steering committee;
- participation from IT, users, consultants, legal and other interested parties, each with a defined set of responsibilities with respect to the acquisition; and
- compatibility with the organisation's acquisition policies and procedures, including any applicable regulatory guidelines.

Documentation and Document Retention Policies

Control objective

8.23 Documentation should be maintained up to date and documentation retention policies should be in place in an organisation. When reviewing an organisation's system of internal control, the IT auditor can gain much of the information required from client documentation.

Risk areas

8.24 The risks associated with inadequate documentation policies include:

unauthorised working practices being adopted by IT staff;

increase in the number of errors being made by IT staff;

the risk of system unavailability in case the system is complex and there is no technical documentation. For example, if an organisation's network is not adequately documented and a problem occurs with the physical layer, those responsible for carrying out repairs would have difficulty in locating where the fault had occurred.

Audit procedure

8.25 The auditor may also need to examine client documentation to test check individual transactions and account balances. The policy on documentation should state that all system documentation should be kept up to date and that only the latest versions should be used. The policy may also state that backup copies of documentation should be stored in a secure off-site location.

Document Retention Policies

8.26 The auditor may need to examine evidence in order to reach an opinion on the financial statements or otherwise. Historically, this evidence has been obtained from paper documents (invoices, purchase orders, goods received notes etc). As more organisations install computer systems, the auditor will find more evidence in the form of electronic records.

8.27 Ultimately, if the organisation does not retain sufficient, appropriate evidence the auditor would have difficulty in being able to provide an unqualified audit opinion.

8.28 The auditor should consider two types of documentation according to the audit approach:

8.29 ***Controls reliant audit approach***: the auditor would require evidence of controls in operation during the accounting period. This evidence may consist of reconciliations, signatures, reviewed audit logs etc.

8.30 ***Substantive testing***: assurance may require the auditor to examine evidence relating to individual transactions. The audit may need to be able to trace transactions from initiation through to their summarisation in the accounts. Where transaction details are recorded in computer systems they should be retained for audit inspection. If the organisation archives data, the auditor may need to ask for it to be retrieved before commencing the audit analysis. If the organisation summarises transactions into balances the auditor will need to find or request an alternative audit trail, e.g. asking the organisation to produce a hard copy of the transactions which make up the summarised balances.

8.31 There may be other, non-audit requirements which require the organisation to retain transaction documentation, e.g.:

import regulations;

taxation regulations; and

company legislation requirements

The organisation's documentation retention policies should take account of all such requirements.

Internal Audit Involvement

Control Objective

8.32 Management has the ultimate responsibility of ensuring that an adequate system of internal controls is in place. Management puts policies and procedures in place and gets assurance that the controls are in place and adequately reduce identified risks by relying on the review work carried out by internal auditors.

Risk Areas

8.33 Basic risk areas which the external auditor may come across when reviewing internal audit's work include:

Internal audit not reporting to senior management.

Management not required to act on internal audit's recommendations.

Internal Auditor may not be empowered to carry out a full range of assessments or there may be significant restrictions on the scope of its work

Non-availability of sufficient resources, in terms of finances and staff.

Audit Procedure

8.34 The external auditor may assess about the quality of internal audit's work acceptable, in terms of planning, supervision, review and documentation.

8.35 The external auditor can view the organisation's internal audit function as part of the overall control structure (since they prevent, detect and correct control weaknesses and errors).

8.36 The external IT auditor should carry out a general assessment of the organisation's internal audit function. This assessment will enable the auditor to decide if we can use or place reliance on internal audit's work. The external IT auditor should determine if:

assurance can be taken from the internal audit activities;

internal audit staff can be used to provide direct audit assistance, if necessary under the supervision of the external auditor. For example, the external auditor may ask the internal auditors to assist with checking the existence of fixed assets.

Before placing reliance on the IT controls review work carried out by the organisation's internal audit, we should carry out our own assessment of their work. This assessment may be largely informed by past experience and direct examination of internal audit's work.

8.37 Staff with IT audit skills and experience will not always be employed by internal audit departments. Some internal audit departments may have in-house IT audit staff; others may contract in IT auditors for specific reviews. Some internal audit departments may not carry out any IT controls reviews.

8.38 The external auditor should consider whether the IT audit department has the staff necessary to carry out competent reviews on the organisation's computer systems.

Legal and Regulatory Compliance

Control Objective

8.39 The legal and regulatory requirements will vary from one country to another. Legal and regulatory requirements may include:

data protection and privacy legislation to protect personal data on individuals, e.g. their payroll information;

computer misuse legislation to make attempted computer hacking and unauthorised computer access a criminal offence;

banking and finance regulations, where banks may have to undergo regular reviews if they wish to continue operating; and

copyright laws to prevent theft & illegal copying of computer software.

Risk Areas

8.40 Non-compliance could result in action varying from a warning letter to prosecution or even closure of the activity being undertaken by the entity.

Audit Procedure

8.41 It may be assessed whether the organisation is aware of local requirements and have taken appropriate measures to ensure compliance.

Personnel and Training

Control Objective

8.42 To ensure that organisation has controls and procedures in place to reduce the risk of mistakes being made. This may be achieved through the adoption of appropriate personnel policies and procedures. Few examples of these are as under:

a clear organisational structure supported by reporting lines/ charts;

job descriptions;

staff planning;

training and staff development;

hiring/firing policies (including codes of conduct);

staff assessments (promotion/demotion);

special contracts;

job rotation

Risk Areas

8.43 In the absence of strong personnel and training control mechanism, there may be repeated instances of data losses, unauthorised data and program amendment, and system crashes attributable to:

- Errors and omissions caused by people;
- Fraud; and
- Hardware/software failure.

Audit Procedure

8.44 Errors and omissions are the biggest source of problems. It is therefore important that the organisation has controls and procedures in place to reduce the risk of above mentioned instances to occur.

Organisational Structure

8.45 There should be a clear organisational structure which shows lines of reporting and management. This should ensure that all staff know how they fit in to the organisational structure of the business and the IT department. The charts also provide an indication of who should be informed when the staff encounter problems.

Job Descriptions

8.46 All IT staff should be given job descriptions. These should describe what tasks the IT staff should perform as part of their jobs. They can be used for staff evaluation and assist the auditor in determining whether there is adequate segregation of duties.

Staff Planning

8.47 Staff planning is important to ensure that there are enough appropriately skilled IT personnel to run the current systems as well as meet future staffing requirements. Examples of the need for staff resource planning include:

where an organisation has decided to upgrade their computer systems, staff who are considered to be experts in the old system may feel that their value to the organisation has diminished or even that their days of employment are numbered. Consequently they may feel demoralised and may not support the old systems adequately;

when installing new systems the technical skill necessary to run the new system may not be available. Management may need to identify skills requirements up front and send staff on training courses, recruit new staff or hire consultants for a period.

Training and Staff Development

8.48 Staff training and development are closely linked to staff resource planning. IT management should know what staff skills are required in both the present and the

foreseeable future. Staff should be given the training to meet those requirements. The need for training is ongoing as both hardware and software continually develops. IT training is often costly and should be controlled by training plans and budgets.

Staff Recruitment/Termination Policies and Codes of Conduct

8.49 The policies should apply to the employment of permanent staff, temporary staff, contractors and consultants. Staff hiring policies should be adopted to ensure that appropriate staff is chosen. There should also be policies and procedures to deal with the other end of the employment cycle, i.e. termination (whether voluntary or compulsory). The policies are likely to be heavily influenced by legal requirements, i.e. the employment legislation within each country.

8.50 When hiring new members of IT staff, the organisation would be expected to take account of:

background checks - including taking up references (in some countries it may be possible to check for criminal convictions);

confidentiality agreements - these state that the employee will not reveal confidential information to unauthorised third parties; and

codes of conduct, including contractual relationships with relatives, the acceptance of gifts, conflicts of interest etc.

8.51 New employees should be made aware of their roles and responsibilities in respect of security matters.

8.52 Termination policies should define the steps to be taken when an employee's services are no longer required. It is important that these policies and procedures are in place because of the considerable damage a disgruntled employee can cause to a computer system.

Staff Assessment

8.53 Staff assessment policies and procedures should be seen to be fair and equitable and understood by all employees. The policies should be based on objective criteria and consideration should be given to all relevant factors, which may include: the staff member's education, training, experience, level of responsibility, achievement, and conduct.

Special Contracts

8.54 It is increasingly common for IT departments to call in specialists, contractors and consultants for one off jobs. There should be policies which require those on special contracts to adhere to established policies and procedures.

Job Rotation

8.55 Job rotation can provide a degree of control because the same person does not carry out the same duties all the time. Job rotation allows other staff to perform a job normally carried out by another person and can lead to the detection and identification of possible irregularities. Job rotation also acts as a preventive control. Staff is less

inclined to adopt unapproved working practices or commit frauds if they know someone else is taking over the job.

Segregation of Duties

Control Objective

8.56 Segregation of duties is a proven way of ensuring that transactions are properly authorised, recorded, and that assets are safeguarded. Separation of duties occurs when one person provides a check on the activities of another. It is also used to prevent one person from carrying out an activity from start to finish without the involvement of another person.

Risk Areas

8.57 Inadequate segregation of duties increases the risk of errors being made and remaining undetected, fraud and the adoption of inappropriate working practices. Separation of duties is a fundamental control requirement as it reduces the risk of error and fraud. This can be achieved through the existence of, and compliance with, job descriptions. Computer systems may be able to enforce separation of duties through the use of pre-programmed user and group security profiles.

Audit Procedure

8.58 Evidence of separation of duties can be obtained by obtaining copies of job descriptions, organisation charts and observing the activities of IT staff. Where computer systems use security profiles to enforce separation of duties, the auditor should review on-screen displays or printouts of employees' security profiles in relation to their functional responsibilities.

8.59 The ability to apply and enforce adequate separation of duties is largely dependent upon the size of the IT department and the number of computer staff involved. Lack of segregated duties in a small computer department can be addressed by compensating controls, e.g. regular management checks and supervision, the use of audit trails and manual controls. However, in a large computer department, the following IT duties should be adequately segregated:

systems design and programming;

systems support;

routine IT operations;

data input;

system administration;

system security;

database administration; and

change management.

8.60 In addition to segregated duties within the IT department, there should be no staff with dual IT department and finance department duties. The computer

department should be physically and managerially separate from end users, such as finance and personnel. Segregation of duties reduces the risk of fraud since collusion would be required to bypass the control.

8.61 Separation of duties applies to both the general controls environment and to specific applications or programs. Within the general IT controls environment, the various functions and roles within the IT department should be segregated.

8.62 For example, a software developer should not require access to the live computing environment to be able to carry out his or her job. Programming staff should not have the authority to transfer new software between the development, test and production environments. Segregation of duties between programmers and operations staff would reduce the risk of those with programming knowledge being able to make unauthorised amendments to programs or data.

8.63 In many cases, the IT department will be divided into two broad types of activity:

programming (systems and applications); and

computer operations

8.64 Staff should not have duties which fall into both types of activity. Programming staff should not be allowed access to live data files and programs.

8.65 With the pressure to reduce the cost of IT functions, staff numbers are often reduced. This limits the scope for segregated duties. If this is the case, then the auditor should adopt a pragmatic approach to identifying weaknesses and providing recommendations. Where the scope for segregated duties is limited the auditor should look for the existence of compensating controls such as strong computer security and end user reconciliations.

8.66 The auditor should determine if IT staff also has responsibilities in user departments. IT should be segregated from user functions such as finance, stock management, grant assessment etc. Staff with duties in both IT and a user area would have greater knowledge of the systems, including the existence of manual and compensating controls, and be able to make unauthorised changes which would be difficult to detect.

IT Operations Controls

Control Objective

8.67 The roles of IT operations include the following:

- ***capacity planning***: i.e. ensuring that the computer systems will continue to provide a satisfactory level of performance in the longer term. This will involve IT operation staff having to make estimates of future CPU requirements, disk storage capacity and network loads capacity.

- ***performance monitoring***: monitoring the day to day performance of the system in terms of measures such as response time.
- ***initial program loading***: booting up the systems, or installing new software.
- ***media management:*** includes the control of disks and tapes, CD ROMs, etc.
- ***job scheduling:*** a job is normally a process or sequence of batch processes which are run overnight or in background and which update files etc. Jobs are normally run periodically, either daily, weekly, monthly, quarterly or annually.
- ***back-ups and disaster recovery***: backups of data and software should be carried out by IT operations staff on a regular basis. Back-up and business continuity issues are covered in depth in a later session.
- ***help desk and problem management***: help desks are the day-to-day link between users with IT problems and the IT department. They are the ones users call when they have a printer problem or they forget their password. Problems may be encountered with individual programs (applications and system), hardware, or telecommunications.
- ***maintenance***: of both hardware and software.
- ***network monitoring and administration***: The IT operations function is given the responsibility for ensuring that communication links are maintained and provide users with the approval level of network access. Networks are especially important where the organisation uses EDI.

8.68 'Computer operations' refers to the logistic and infrastructure aspects of hardware and software. Appropriate computer operations shield users from the need to consider these matters by ensuring that the application systems are available at scheduled times, they operate as expected and the results of their processing, such as printouts, are produced on time. In a well run IT department, we expect to find computer operations that are transparent to users, fully supporting them in the performance of their roles.

Risks Areas

8.69 The risks associated with poorly controlled computer operations are:

applications not run correctly **(wrong applications run, or incorrect versions or wrong configuration parameters entered by operations staff, e.g. the system clock and date being incorrect which could lead to erroneous interest charges, payroll calculations etc);**

loss or corruption of financial applications **or the underlying data files: may result from improper or unauthorised use of system utilities. The IT operations staff may not know how to deal with processing problems or error reports. They may cause more damage then they fix;**

delays and disruptions in processing**. Wrong priorities may be given to jobs;**

lack of backups and contingency planning **increases the risk of being unable to continue processing following a disaster;**

***lack of system capacity*. The system may be unable to process transactions in a timely manner because of overload, or lack of storage space preventing the posting of any new transactions;**

***high amount of system downtime* to fix faults: when the systems are unavailable a backlog of un-posted transactions may build up; and**

***users' problems remaining unresolved* due to a poor help-desk function. Users may attempt to fix their own problems.**

Audit Procedures

Service Level Agreements

8.70 It is increasingly common for IT departments to draw up and enter into service level agreements (SLA) with the rest of the organisation, i.e. the user departments. This allows users to specify and agree, preferably in writing, what levels of service, in terms of quantity and quality, they should receive. SLAs are in effect internal service delivery contracts.

8.71 The structure and level of service specified in a SLA will depend upon the working practices and requirements of each organisation. A typical SLA would contain the following:

general provisions (including the scope of the agreement, its signatories, date of next review);

brief description of services (functions applications and major transaction types);

service hours (normal working hours and special occasions such as weekends and holidays);

service availability (percentage availability, maximum number of service failures and the maximum downtime per failure);

user support levels (help desk details);

performance (response times, turnaround times);

contingency (brief details of plans);

security (including compliance with the organisation's IT security policy); and

restrictions (maximum number of transactions, users);

The auditor should review any SLA to determine that they support the accurate and consistent processing of financial data.

Outsourcing Policy

8.72 There is an increasing trend for IT services to be delivered by third party service providers. This has arisen because IT is not seen as being a core business activity. By the late 1990s, IT outsourcing had become a mainstream management option and outsourcing contracts are now quite common in auditee organisations.

Management may take the attitude that their business involves the delivery of products and services, and not the provision of IT services.

Control Objective

8.73 Outsourcing allows management to concentrate their efforts on the main business activities as the need for developing and maintaining the IT Systems are taken care of by the IT expert third parties/agencies.

Risk Areas

8.74 The decision of outsourcing any business activity, may have the basic intentions of allowing the Top Management to concentrate more upon the main business activities, however, this involves invitation to the risk of allowing a third party to have access to the business secrets, important data and other related facts.

Audit Procedure

8.75 Where an organisation does outsource or intends to outsource its IT activities the auditor should be concerned with reviewing the policies and procedures which ensure the security of the organisation's financial data. The auditor may need to obtain a copy of the contract to determine if adequate controls have been specified. Where the organisation intends to outsource its IT function the auditor should ensure that audit needs are taken into account and included in contracts. Contract terms are frequently difficult to change once they have been signed. Even if the third party is willing to amend the contract it is likely to charge a large fee for doing so.

Problems in Outsourcing

8.76 Organisations, particularly those in developing countries and those with little relevant previous experience, may inadvertently create various problems when they decide to outsource their system development and software implementation projects. These may include:

- The price of the software to be implemented often appears to be the deciding factor in choosing the outsourcing vendor rather than the overall potential result for the organisation.
- The organisation generally has little or no clear plan of what it wants done. There are no clear ideas on reporting requirements and, at times, very little in the way of specified or defined systems. Most of the time, the development work is undertaken with systems, procedures and controls evolving alongside.
- Management does not really know what platforms may be best suited for the proposed development work.
- Top management is, or regards itself as being, too busy to be trained in the software to be used. This has a debilitating effect on the rest of the staff. Success of the project depends on significant participation by top management.
- Where activities are outsourced, management and users may sometimes expect far more than is really possible. They may have an unrealistic expectation of

the value to be expected for the payment being made. For example, even though the basic payroll or accounts may be produced in a timely and cost-effective fashion, users may also expect complex and unspecified information reports that, in fact, are not produced and never could be for the contract price of the service.

8.77 The IT auditor should also focus on issues related to IPR (Intellectual Property Rights) and evaluate whether the programs etc. developed by outsourcing components to a third party are duly protected as per contract terms and are not prone to outside use by other organisations.

Management Control, Review and Supervision

8.78 Operations staff should be supervised by the management. From the standpoint of separation of duties, operations staff should not be given the job of inputting transactions or any form of application programming.

8.79 The organisation's IT systems may have on them software utilities which could conceivably be used to make unauthorised amendments to data files. Operations staff with access to such software should be supervised to ensure that they only use the utilities for authorised purposes.

8.80 Management will be unable to provide continuous monitoring of operations staff and may place some reliance on the automatic logging and monitoring facilities built into the systems. The events which are recorded in the logs will depend on the parameters set when the systems were installed. As with most logging systems, a large quantity of data can be produced in a short period.

8.81 Recommending that an organisation review the audit logs on a regular basis is unlikely to be carried out in practice. To assist management in their detection of unauthorised activity, the organisation should develop procedures (e.g. a program) to report exceptions or anomalies.

8.82 Effective supervision over IT operations staff is often difficult to achieve, due to their high level of technical knowledge. They could do things to the system which management would not detect, or even recognize the significance of, if they did detect a change. Therefore, to a certain extent management must place a high degree of trust on IT operations staff, and that trust will be based on appropriate staff selection and vetting procedures (as per the organisational and management controls discussed in the previous topic).

Training and Experience

8.83 IT operations staff should have skills, experience and training necessary to carry out their jobs to a competent standard. The IT auditor should determine if the training needs of IT operations staff have been assessed. Training needs may include non-technical training, e.g. management training for IT operations supervisors.

8.84 As an aid to continuity of staffing, some organisations may teach staff more than one role or introduce a form of job rotation.

8.85 Closely connected to training is the career development of staff. If IT operations feel that they are in a dead end job with little scope for progression their morale may be low and they are less likely to carry out their work to a high standard.

Computer Maintenance

8.86 As with most equipment, computers may require regular maintenance to reduce the risk of unexpected hardware failures. Although preventive maintenance is becoming less common, especially for mini and microcomputers, it may still be required for environmental equipment such as air conditioning units and fire extinguishing systems. The IT operations function should either have an internal maintenance capability, or contract out the maintenance to a third party supplier.

8.87 The IT auditor may wish to examine the maintenance contracts and schedules to determine if adequate maintenance is carried out. Ultimately the key test to the adequacy of the organisation's maintenance arrangements is the amount of system down-time or the number of Helpdesk incidents arising from equipment failures.

Operations Documentation

8.88 The organisation should have clear, documented operating procedures for all computer systems to ensure their correct, secure operation. The documented procedures should be available for the detailed execution of each job, and should include the following items:

the correct handling of data files;

scheduling requirements (to ensure best use of IT resources);

instructions for handling errors or other exceptional conditions which might arise when jobs are run;

support contacts in the event of unexpected operational or technical difficulties;

special output handling instructions; and

system restart and recovery procedures.

8.89 The organisation should also have documented procedures for daily housekeeping and maintenance activities such as computer start-up procedures, daily data back-up procedures, computer room management and safety.

8.90 Documentation can be used by operations staff when they are unsure about how to carry out a procedure. They are also useful in training new staff.

8.91 The auditor should bear in mind the level and detail of documentation will vary from one organisation to another, and will depend on factors such as the size of the organisation, the type of hardware and software used and the nature of the applications. The auditor would expect to see large quantities of high quality documentation in a large, critical IT operation, whereas a small organisation running office automation software would probably have less detailed and extensive documentation.

Problem Management

8.92 The IT operation section should have documented procedures for detecting and recording abnormal conditions. A manual or computerised log may be used to record these conditions.

8.93 The ability to add an entry to the log should not be restricted; however the ability to update the log should be restricted to authorised personnel only. Management should have mechanisms in place to ensure that the problem management mechanism is properly maintained and that outstanding errors are being adequately addressed and resolved.

Network Management and Control

8.94 A range of controls is required where an organisation uses computer networks. Network managers should ensure that there are appropriate controls to secure data in networks, and that the network is adequately protected from unauthorised access. The controls may include:

separation of duties between operators and network administrators;

establishment of responsibility for procedures and management of remote equipment;

monitoring of network availability and performance. There should be reports and utilities to measure system response time and down time; and

establishment and monitoring of security controls specific to computer network.

Summary

8.95 The IT auditor may be required to review the security and controls in non-financial systems and financial systems, depending on the scope of an audit and each SAI's mandate.

Physical Controls (Access and Environmental)

Control Objective

8.96 The objective of physical and environmental controls is to prevent unauthorised access and interference to IT services. In meeting this objective, computer equipment and the information they contain and control should be protected from unauthorised users. They should also be protected from environmental damage, caused by fire, water (either actual water or excess humidity), earthquakes, electrical power surges or power shortages. In IT arena, the second most likely cause of errors is natural disasters. The entity's IT security policy should include consideration of physical and environmental risks.

Risks Areas

8.97 **Physical**

Accidental or intentional damage by staff.

Theft of computers or their individual components (computer theft is on the increase and is likely to continue. Consider that, weight for weight, computer chips are worth more than gold and are very attractive to thieves);

Power spikes or surges which may cause component damage and the loss or corruption of data;

Bypass of logical access controls: e.g. having physical access to a fileserver can be exploited to bypass logical controls such as passwords; and

Copying or viewing of sensitive or confidential information, e.g. pricing policies, pre-published results, and government policies.

8.98 **Environmental**

Fire/water damage (or damage from other natural disasters);

Power: Cuts, leading to loss of data in volatile storage (RAM);

Spikes: leading to system failures, processing errors, damage to components of equipment.

Failure of equipment due to temperature or humidity extremes (or just outside tolerances of a few degrees);

Static electricity: can damage delicate electrical components. Computer chips (ROM, RAM and processor) are delicate and easily damaged by static electricity shocks;

Others: e.g. lightning strikes, etc.

8.99 Some of these risks are also covered in greater depth in the Business Continuity Planning of this manual.

Audit Procedure

8.100 To ensure that adequate internal controls exist to protect the business's assets and resources, the organisation should carry out a risk assessment. This would involve identifying the threats to the systems, the vulnerability of system components and likely impact of an incident occurring. Then he should identify counter-measures to reduce the level of exposure to an acceptable level. To do this, he must balance the risks identified with the cost of implementing controls. Some controls would be expensive to implement and would only be justified in a high risk environment.

8.101 The counter measures, or controls that the entity puts in place will vary from one organisation to another. For example, a large government department with its own data centre will usually have a higher degree of controls over its IT facilities than a small organisation using office automation systems such as word processing and spreadsheets.

Physical Controls

8.102 Physical access controls are specifically aimed at ensuring that only those who have been authorised by management have physical access to the computer systems.

Physical access security should be based upon the concept of designated perimeters which surround the IT facilities.

8.103 Physical access controls reduce the risk of unauthorised persons gaining access to the computer equipment. The auditor should identify controls which would restrict access to the organisation's site, the computer rooms, terminals, printers and data storage media. The organisation should also have considered the risks posed by cleaners, security personnel and maintenance staff. Common physical access controls include the use of locked doors, CCTV, intruder alarms, combination keypads and security guards.

8.104 Access to the organisation's site and secure areas should be controlled by layers of controls, starting at the perimeter fence and working in through the building's entrance to the computer suite and terminals. Physical controls may be explicit, such as a door lock; or implicit for example an employees' job description implies a need to enter the IT operations area.

☞ Newer devices such as biometric devices use voice recognition, facial features, hand geometry, fingerprints, retina scan etc to control physical access to the system. The process is of two types

- One to many, where the biometric input is compared with the data available in the system to recognize the person and to give access.
- Many to one, where the identity of the person is disclosed first and then the biometric input is compared to the specific data relating to that identity.

Security of Biometric data is of paramount importance to prevent unauthorised access and crime due to impersonation.

8.105 Computer installations should be protected against hazards such as fire, flood, power cuts, physical damage and theft. Inadequate protection increases the risk to system availability and ultimately an organisation's ability to produce a complete record of financial transactions. The organisation should have assessed the exposure to damage and introduced appropriate controls to reduce the risk to an acceptable level.

8.106 The risk of fire damage can be reduced by the provision of fire detection and fire fighting equipment. Other measures, such as regular cleaning and removal of waste from the computer room, will reduce the risk of fire damage.

8.107 The risk of water damage is largely dependent on the location of the computer facilities. Equipment located in close proximity to pipes and water tanks are at increased risk. Where possible, organisations should avoid locating computer equipment in basements or on floors immediately below or in the vicinity of water

tanks. Automatic moisture detectors may be used to alert IT staff of potential water ingress.

8.108 Computer equipment may be damaged or disrupted by fluctuations in the electrical power supply. Power surges can cause computer systems to delete or contaminate data. Uninterruptible power supplies reduce the risk of system disruption and damage and can allow continued processing following a power cut.

8.109 Some of the older and larger computer installations require special environmental controls to regulate both the temperature and humidity in their vicinity. These controls usually take the form of air conditioning units. Many of the latest generation mini and micro computers have been designed to operate in an office environment and hence will not require special environmental controls.

Logical Access Controls

8.110 Logical access controls are defined as: "a system of measures and procedures, both within an organisation and in the software products used, aimed at protecting computer resources (data, programs and terminals) against unauthorised access attempts."

Control Objective

8.111 The objective of logical access controls is to protect the financial applications and underlying data files from unauthorised access, amendment or deletion. The objectives of limiting access are to ensure that:

- Users have only the access needed to perform their duties
- Access to very sensitive resources such as security software program, is limited to very few individuals, and
- Employees are restricted from performing incompatible functions or functions beyond their responsibility

8.112 **Risk Areas**

- Users have the access to the areas other than related to the performance of their duties, causing threats to unauthorised access, amendment or deletion in the maintained data.
- Access to very sensitive resources such as security software program which may be of mission critical nature, and
- Employees are not barred/ restrained from performing incompatible functions or functions beyond their responsibility.

Audit Procedure

8.113 Logical access controls can exist at both an installation and application level. Controls within the general IT environment restrict access to the operating system,

system resources and applications, whilst the application level controls restrict user activities within individual applications.

8.114 The importance of logical access controls is increased where physical access controls are less effective, for example, when computer systems make use of communication networks (LANs and WANs). The existence of adequate logical access security is particularly important where an organisation makes use of wide area networks and global facilities such as the Internet.

8.115 Logical access controls usually depend on the in-built security facilities available under the operating system (e.g. NOVELL Network) or hardware in use. Additional access controls can be gained through the appropriate use of proprietary security programs.

8.116 The most common form of logical access control is login identifiers (ids) followed by password authentication. For passwords to be effective there must be appropriate password policies and procedures, which are known to all staff and adhered to. Organisations may be able to tailor the password system by, for example, setting minimum password lengths, forcing regular password changes and automatically rejecting purely numerical passwords, peoples' names, or words which appear in the English dictionary.

8.117 Menu restrictions can be effective in controlling access to applications and system utilities. Systems may be able to control access by identifying each individual user through their unique login ids and then having a pre-defined profile of authorised menus for each. The auditor should consider how easy it would be for users to 'break out' of the menu system and gain unauthorised access to the operating system or other applications.

8.118 Some computer systems may be able to control user access to applications and data files by using file permissions. These ensure that only those users with the appropriate access rights can read, write, delete or execute files.

8.119 Significant risks are often posed by system administration staff with powerful system privileges. These 'super users' may have access to powerful system utilities that can by-pass established system controls. Management should have introduced measures to control the activities of these powerful users and, if possible, limit the system privileges of individual administrator to those required by their function.

8.120 The auditor should bear in mind that some operating systems and associated logical access control options, file parameters, etc., are very technical in nature. Where the organisation's systems are technically complex and the auditor does not have a working knowledge of the organisation's particular systems, the IT auditor may need to obtain additional support and assistance from an IT auditor with the relevant skills and experience.

8.121 The critical elements of an access control mechanism should include:

- Classification of information resources according to their criticality and sensitivity

- Maintenance of a current list of authorised users and their access privileges
- Monitoring access, investigating apparent security violations, and take appropriate remedial action.

Resources, Files and Facilities requiring Protection

Data Files

8.122 These may consist of transaction files or databases. Any files containing master file or standing data information should also be protected, e.g. files containing payroll rates, bank account codes system parameters etc. If not protected someone could make unauthorised amendments or even delete the data.

Applications

8.123 Unrestricted access increases the risk that the applications will be subject to unauthorised amendment leading to fraud, data loss, and corruption. Unauthorised access to the source code of an application could be used to make amendments in the programming logic, e.g. rounding off payments to the nearest unit (paisa) and posting the rounded fraction to the programmer's expense repayment account.

8.124 Where a system carries out complex calculations it may not be possible to independently check the applications calculations and unauthorised amendments may remain undetected for a considerable time.

Password Files

8.125 If these files are not adequately protected and anyone can read them there would be little to stop an unauthorised person obtaining the logon identification and password of a privileged system user. Any unauthorised user who obtained the access permissions of a privileged system user would be able to cause considerable damage.

8.126 Even where the identifier and password of an ordinary user are obtained, the concept whereby users are held accountable for their actions is bypassed. The unauthorised user could use the "stolen" identification to make amendments which cannot be traced back to the perpetrator or use it as a stepping stone to obtain higher access privileges.

System Software and Utilities

8.127 These consist of software such as editors, compilers, program debuggers. Access to these should be restricted as these tools could be used to make amendments to data files and application software.

Log Files

8.128 Log files are used to record the actions of users and hence provide the system administrators and organisation management with a form of accountability. A system log can record who logged onto the system and what applications, data files or utilities they used whilst logged on. An application log can be used to record changes to financial data (who changed what data, from what to what and when). If log files are

inadequately protected, a hacker, fraudster etc. could delete or edit it to hide his/her actions.

Program Change Controls

Control Objective

8.129 Even when the system development process has been completed and the new system is accepted, it is likely that it will have to be changed, maintained, or altered during its lifecycle. This change process may have an impact on the existing controls and may affect the underlying functionality of the system. If the auditor intends to rely on the system to any extent to provide audit evidence, a review of the change controls is required. Change controls are needed to gain assurance that the systems continue to do what they are supposed to do and the controls continue to operate as intended.

8.130 Change refers to changes to both hardware and software. Hardware includes the computers, peripherals and networks. Software includes both the system software (operating system and any utilities) and individual applications.

8.131 The scale of change can vary considerably, from adjusting a system's internal clock, to installing a new release of an application or operating system. The effect that a change has on the operation of the system may be out of proportion to the size or scale of the change made.

Reasons for System Changes

8.132 After systems are implemented the system maintenance phase begins. Systems rarely remain the same for long. Even on the day systems go live there are invariably users who are not satisfied with the systems and submit request for changes (RFC) to be made.

8.133 Changes may be requested for the following reasons:

To enhance functionality: everyday system users may not be content with the functionality of the system. This could include discontentment with the screens they have, the system response time. Users may also identify bugs in programs which cause the system to produce erroneous results;

To make systems operations easier, more efficient: this category includes the tape/disk operators, the Helpdesk manager, the database administrator and network management personnel;

Capacity planning: the system may require additional resources or increased capacity components e.g. a more powerful CPU to cope with increased processing demand, or additional disk drives as the existing drives fill up;

Problem rectification: helpdesk incidents leading to the identification of problems: each incident recorded on the Helpdesk will contribute to the identification of underlying problems. If the problems are significant enough a request for change may be produced by the Helpdesk function;

To improve security: IT security personnel: identified weaknesses in system security may result in requests for change which should improve security;

Routine updates: system developers may update and improve the system software. They may also request changes when software suppliers "insist" that the organisation runs the current version of their software; or

Changes in requirements: changes in legislation, business requirements or business direction may require the financial system to be amended.

Risk Areas

8.134 Change controls are put in place to ensure that all changes to systems configurations are authorised, tested, documented, controlled, the systems operate as intended and that there is an adequate audit trail of changes.

8.135 Conversely, the risks associated with inadequate change controls are as follows:

***Unauthorised changes*: accidental or deliberate but unauthorised changes to the systems. For example, if there are inadequate controls application programmers could make unauthorised amendments to programs in the live environment;**

***Implementation problems*: for example where the change is not in time for business requirements, e.g. annual tax rates;**

***Erroneous processing, reporting*: systems which do not process as intended. This could lead to erroneous payments, misleading reports, wrong postings of transactions and ultimately qualified accounts;**

***User dissatisfaction*: systems which users are not happy with: this could lead to data entry errors, staff morale problems, a loss of productivity, union actions;**

***Maintenance difficulties*: poor quality systems, which are difficult or expensive to maintain (e.g. due to a lack of system documentation). Where there are inadequate controls over changes there could be multiple changes to the system so that nobody is sure which versions of software, or modules are being used in the live environment. Nobody would know which bugs had been fixed, or what parameters have been altered in different versions;**

***Use of unauthorised hardware and software*: systems (hardware and software) in use which are not authorised. This could lead to incompatibility between different parts of the system, or breach of copyright legislation; and**

***Problems with emergency changes*: uncontrolled emergency changes to programs in the live environment leading to data loss and corruption of files.**

Audit Procedure

8.136 It may be ensured in audit that the organisation's procedures to control changes should include:

Procedures for management authorisation;

Thorough testing before amended software is used in the live environment;

The amended software is transferred or "transported" to the live environment only by or often authorised by operations management;

Management review of the effects of any changes;

Maintenance of adequate records;

The preparation of fallback plans (just in case anything goes wrong); and

The establishment of procedures for making emergency changes.

8.137 There should be procedures for recording all requests for change (RFC), preferably in a standard format and/or data input screens. The requests for changes should be logged and given a unique chronological reference number. All RFCs should be allocated a priority rating to indicate the urgency with which the change should be considered and acted upon. The task of determining change priority is normally the responsibility of a change control board or IT steering committee. The change board and steering committee make their views known via an individual given the role of the change manager. The priority of changes is determined by assessing the cost of the change and impact on the business and its resources.

Business Continuity and Disaster Recovery Controls

Control Objective

8.138 The objective of having a Business Continuity and Disaster Recovery Plan and associated controls is to ensure that the organisation can still accomplish its mission and it would not loose the capability to process, retrieve and protect information maintained in the event of an interruption or disaster leading to temporary or permanent loss of computer facilities.

Risks Areas

8.139 The absence of a well defined and tested Business Continuity and Disaster Recovery Plan may pose the following major threats to the very existence of the organisation in the event of a disaster:

- The organisation's ability to accomplish its mission after re-starting its operations.
- To retrieve and protect the information maintained.
- To keep intact all the organisational activities after the disaster.
- To start its operations on full scale at the earliest to minimise the business loss in terms of money, goodwill, human resources and capital assets.

Audit Procedures

8.140 The organisation with computerised systems should have assessed threats to the system, its vulnerability and the impact a loss of operations would have on the

organisation's ability to operate and achieve organisational objectives. Appropriate measures should then be put in place to reduce risks to a level that is acceptable to the organisation's senior management.

8.141 The extent of business continuity and disaster recovery planning and the detailed measures required will vary considerably. Organisations with large IT departments, with mainframe computers and complex communication networks may require comprehensive, up to date continuity and recovery plans which incorporate standby facilities at alternative sites. At the other end of the scale, a small agency or non-departmental public body with a desk-top PC, running a simple off the shelf package, would have a simpler plan.

8.142 Continuity and disaster recovery plans should be documented, periodically tested and updated as necessary. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

8.143 The importance of adequate documentation is increased where significant reliance is placed on a few key members of the IT department. The loss of key staff, perhaps due to the same reason the computers were disrupted, may adversely affect an organisation's ability to resume operations within a reasonable timeframe.

8.144 Back-up copies of systems software, financial applications and underlying data files should be taken regularly. Back-ups should be cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back-ups should be stored, together with a copy of the disaster recovery plan and systems documentation, in an off-site fire-safe.

8.145 The IT auditor while assessing the adequacy of business continuity and disaster recovery plan should consider:

- Evaluating the business continuity and disaster recovery plans to determine their adequacy by reviewing the plans and comparing them to organisational standards and/or government regulations.
- Verifying that the business continuity and disaster recovery plans are effective to ensure that information processing capabilities can be resumed promptly after an unanticipated interruption by reviewing the results from previous tests performed, if any, by the IT organisation and the end users.
- Evaluating off site storage to ensure its adequacy by inspecting the facility and reviewing its contents and security and environmental controls. It may be ascertained whether backups taken earlier have ever been tested for data recovery by the auditee organisation.
- Evaluating the ability of IT and user personnel to respond effectively in emergency situations by reviewing emergency procedures, employee training and results of their drills.

9. AUDIT OF APPLICATION CONTROLS

9.1 Application controls are particular to an application and may have a direct impact on the processing of individual transactions. These controls are used to provide assurance that all transactions are valid, authorised, complete and recorded. Since application controls are closely related to individual transactions it is easier to see why testing the controls will provide the auditor with audit assurance as to the accuracy of a particular account balance. For example, testing the controls in a payroll application would provide assurance as to the payroll figure in an organisation's accounts is correct or otherwise

9.2 Before getting on to evaluation of application controls, it will be necessary for an auditor to secure a reasonable understanding of the system. For this purpose, a brief description of the application should be prepared;

- indicating the major transactions,
- describing the transaction flow and main output,
- indicating the major data files maintained and
- providing approximate figures for transaction volumes.

9.3 Application controls may be divided into:

- Input controls
- Processing controls
- Output controls
- Master/Standing Data File controls

☝ *This chapter deals with generic level application controls only. Specific business rules of the organization have to be studied to evaluate corresponding application controls. For example in a housing organization if the rule says that not more than one house can be allotted to an individual then it has to be seen that validation checks are incorporated to prevent duplication or if in an electricity company the rule states that the first bill has to be generated within 30 days of a new connection then this should be incorporated by way of processing logic. This is an area where the institutional knowledge of the audit offices regarding the auditee organizations would be put to maximum use.*

Input Controls

Control Objective

9.4 The objective of Input control is to ensure that the procedures and controls reasonably guarantee that (i) the data received for processing are genuine, complete, not previously processed, accurate and properly authorised and (ii) data are entered accurately and without duplication. Input control is extremely important as the most important source of error or fraud in computerised systems is incorrect or fraudulent input. Controls over input are vital to the integrity of the system.

Risk Areas

9.5 Weak input control may increase the risk of:

- entry of unauthorised data
- data entered in to the application may be irrelevant.
- incomplete data entry
- entry of duplicate/redundant data.

Audit Procedure

9.6 The aspects that the auditor should evaluate are:

- all prime input, including changes to standing data, is appropriately authorised.
- for on-line systems, the ability to enter data from a terminal is adequately restricted and controlled.
- if there is a method to prevent and detect duplicate processing of a source document.
- all authorised input has been submitted or, in an on-line system transmitted and there are procedures for ensuring correction and resubmission of rejected data.

9.7 The controls outlined above may be invalidated if it is possible to by-pass them by entering or altering data from outside the application. There should be automatic application integrity checks which would detect and report on any external changes to data, for example, unauthorised changes made by personnel in computer operations, on the underlying transaction database. The results of the installation review should be reviewed to ensure that the use of system amendment facilities, such as editors, is properly controlled.

Authorisation of Input

9.8 The organisation should have procedures and controls in place to ensure that all transactions are authorised before being entered into the computer system. From the external auditor's point of view authorisation controls reduce the risk of fraudulent, or irregular transactions. The organisation also gains better control of resources.

9.9 Computerised applications may be able to permit staff to enter and authorise transactions directly in the system. This can be achieved by setting up password access controls to data input devices and data entry permissions, e.g. data input screens. Financial applications may be able to check that a transaction has been approved by a person with the appropriate level of authority by checking their log-in ID against a predefined transaction approvals list.

9.10 To place reliance on the automated controls the IT auditor would need to determine that the appropriate levels of authority have been set up and that they have been working for the whole accounting period / transaction cycle. This would involve:

looking at access matrices;

obtaining printout of user permissions;

reviewing audit logs of changes in permissions

Completeness of Input Data

9.11 As part of an IT audit, the auditor must determine if the accounting records are complete and that there are no material omissions. To do this the auditor should review the controls which ensure that input is complete, i.e. that transactions have not gone missing. The completeness of transaction input can be ensured by a variety of controls:

manual procedures e.g. keeping a log of transactions which users send for input. The data input staff in the IT department may expect a regular flow or pattern of transactions from user departments. Where a batch of input documents is expected but not received or a batch number appears to be missing, follow up action should be taken to identify the missing transactions;

the use of pre-numbered data input forms. These may be sequentially numbered. When a number is found to be missing the finance / concerned staff can investigate any disappearances. Alternatively the input transactions may be sent on sequentially numbered batch forms from user departments;

use of batch totals : In a traditional batch input system, all data is presented to the system in batches and incomplete batches are detected and exception reports are produced; and

establishing a routine or expectation of data input e.g. if data entry staff expect to receive input documents from all 10 departments on a particular day and they only receive 9 sets, they would chase up the missing set of input documents.

9.12 A batch is a collection of input documents which are treated as one group. The existence of batches is useful in establishing controls to ensure the completeness of input of data to the system. The total of individual transactions should agree to a manually calculated total recorded for input on a batch header document.

9.13 Batch totals should be recorded at the earliest possible point in the processing cycle and totals agreed from update reports back to this original record, i.e. the first batch total acts as a reference to check back to, as the transactions are processed by the system.

9.14 Control must be exercised by the users to ensure that all batches are processed as well as to ensure that the correct value is accepted for each batch. It is therefore essential that a complete record of all batches sent for processing is maintained. This is usually a log book completed by the computer operators and reviewed and signed by a supervisor.

9.15 More importantly, applications may also have in-built controls to ensure that all the key transaction information has been entered before the transaction can be posted to the accounts. For example if the finance user does not input data in a key field such as **amount** the transaction would be rejected by the system.

Data Input Validation

9.16 IT applications may have in-built controls which automatically check that data input is accurate and valid. Validation may also be achieved by manual procedures such as double checking input documents or review by a supervisor.

9.17 The accuracy of data input to a system can be controlled by imposing a number of computerised validity checks on the data presented to the system. Automated validation checks should be sufficient to ensure that all data accepted into the system is capable of acceptance by all subsequent processes, including acceptance into other systems where there is an automatic transfer of data. Acceptability is particularly important where feeder systems are used. For example the output from a standalone payroll system may provide the input for a general ledger system. Validation checks can reduce the risk of an application crashing because of logic errors arising when attempting to process input data with values outside pre-defined limits.

9.18 There are many types of programmed application control which an IT auditor may encounter. For example: format checks, validity checks, range checks, limit checks, check digits, compatibility checks, etc.

Duplicate Checks

9.19 The increase in the number of transactions that need to be processed has played a large part in the computerisation of accounting and business critical systems. Unfortunately, the increased volume of transactions has resulted in end user staff being less likely to remember transactions they have previously processed. This increases the risk that duplicate transactions will occur and remain undetected.

9.20 To address this risk, some applications may be able to detect duplicate transactions, e.g. by comparing new transactions with transactions previously posted to the same account. An IT auditor can make use of CAATs software to detect the duplicate records in any transaction file.

Matching

9.21 This control checks and compares one transaction record against data contained in another related transaction. Where data is found to differ an exception report is produced. For example, the data entered when goods are received are automatically compared to the supplier's invoice and the purchase order data on the system. Where a mismatch is found the computer produces an exception report. The organisation should then take steps to identify the cause of the discrepancy.

Dealing with Rejected Input

9.22 It is important that, where data is automatically checked and validated at data entry, there are procedures for dealing with transactions which fail to meet the input requirements, i.e. the auditor should determine what happens to rejected transactions.

9.23 There are alternative methods of dealing with input transactions which fail validity tests.

9.24 **Rejected by the system** - Where transactions are rejected outright, the organisation should have procedures in place to establish control over these rejections and ensure that all data rejected will be subsequently corrected, re-input to and accepted by the system. The system rules will determine whether individual transactions or complete batches should be rejected.

9.25 **Held in suspense** - in this case it is critical that users recognize the placing of items in suspense as a prompt for action. It is essential that all items held in suspense are corrected and ultimately successfully processed. In adopting this approach, we overcome the possibility of rejected items being lost but delay the recognition of the need to take action to correct the input error. Where items are held in suspense the auditor should review the procedures for identifying, correcting and clearing these transactions.

Processing Controls

9.26 Processing controls ensure complete and accurate processing of input and generated data. This objective is achieved by providing controls for:

- adequately validating input and generated data,
- processing correct files ,
- detecting and rejecting errors during processing and referring them back to the originators for re-processing,
- proper transfer of data from one processing stage to another, and
- checking control totals (established prior to processing) during or after processing.

Control Objective

9.27 The objectives for processing controls are to ensure that:

- transactions processing is accurate;
- transactions processing is complete;
- transactions are unique (i.e. no duplicates);
- all transactions are valid; and
- the computer processes are auditable.

Risk Areas

9.28 Weak process controls would lead to:

- inaccurate processing of transactions leading to wrong outputs/results.
- some of the transactions being processed by the application may remain incomplete.
- allowing for duplicate entries or processing which may lead to duplicate payment in case of payment to vendors for goods.

- unauthorised changes or amendments to the existing data.
- absence of audit trail rendering, sometimes, the application unauditable.

Audit Procedure

9.29 Processing controls within a computer application should ensure that only valid data and program files are used, that processing is complete and accurate and that processed data has been written to the correct files. Assurance that processing has been accurate and complete may be gained from performing a reconciliation of totals derived from input transactions to changes in data files maintained by the process. The auditor should ensure that there are controls to detect the incomplete or inaccurate processing of input data.

9.30 Application processes may perform further validation of transactions by checking data for duplication and consistency with other information held by other parts of the system. The process should check the integrity of data which it maintains, for example, by using check sums derived from the data. The aim of such controls is to detect external amendments to data due to system failure or use of system amendment facilities such as editors.

9.31 Computerised systems should maintain a log of the transactions processed. The transaction log should contain sufficient information to identify the source of each transaction. In batch processing environments, errors detected during processing should be brought to the attention of users. Rejected batches should be logged and referred back to the originator. On-line systems should incorporate controls to monitor and report on unprocessed or unclear transactions (such as part paid invoices). There should be procedures which allow identifying and reviewing all unclear transactions beyond a certain age.

Output Controls

9.32 These controls are incorporated to ensure that computer output is complete, accurate and correctly distributed. It may be noted that weakness in processing may sometimes be compensated by strong controls over output. A well-controlled system for input and processing is likely to be completely undermined if output is uncontrolled. Reconciliation carried out at the end of the output stage can provide very considerable assurance over the completeness and accuracy of earlier stages in the complete cycle.

Control Objective

9.33 Output controls ensure that all output is:

- produced and distributed on time,
- fully reconciled with pre input control parameters,
- physically controlled at all times, depending on the confidentiality of the document and
- errors and exceptions are properly investigated and acted upon.

Risk Areas

9.34 If output controls prevailing in the application are weak or are not appropriately designed these may lead to:

- repeated errors in the output generated leading to loss of revenue, loss of creditability of the system as well as that of the organisation.
- non-availability of the data at the time when it is desired.
- availability of the data to an unauthorised person/user.
- even sometimes, the information which may be of very confidential nature may go to the wrong hands.

Audit Procedure

9.35 The completeness and integrity of output reports depends on restricting the ability to amend outputs and incorporating completeness checks such as page numbers and check sums.

9.36 Computer output should be regular and scheduled. Users are more likely to detect missing output if they expect to receive it on a regular basis. This can still be achieved where the subject of computer reports is erratic, such as exception reporting, by the production of nil reports.

9.37 Output files should be protected to reduce the risk of unauthorised amendment. Possible motivations for amending computer output include covering up unauthorised processing or manipulating undesirable financial results. Unprotected output files within a bill paying system could be exploited by altering cheque or payable order amounts and payee details. A combination of physical and logical controls may be used to protect the integrity of computer output.

9.38 Output from one IT system may form the input to another system, before finally being reflected in the financial statements, for example, the output from a feeder system such as payroll would be transferred, as input, to the general ledger. Where this is the case the auditor should look for controls to ensure that outputs are accurately transferred from one processing stage to the next. A further example would be where the output from a trial balance is used as the input to a word-processing or spreadsheet package, which then reformats the data to produce the financial statements.

Master/Standing Data File Controls

Control Objective

9.39 Master/Standing Data File controls are meant for integrity and accuracy of Master Files and Standing Data.

Risk Areas

9.40 Accuracy of data on Master and Standing files is of vital importance, to the auditor. Information stored in master and standing data files is usually critical to the processing and reporting of financial and operational data. Information on master files

can affect many related transactions and must therefore be adequately protected. Weak Control in the system in maintenance of Master/Standing Data Files may lead to:

- unauthorised and uncontrolled amendments to the standing data as well as Master data files.
- unrestricted and uncontrolled physical and logical access to the application data files.
- poor documentation of the amendment procedures, etc.

Audit Procedure

9.41 Auditors should see the following while examining the system:

- amendments to standing data are properly authorised and controlled.
- integrity of Master and Standing Files is verified by checking, control totals and periodic reconciliation with independently held records.
- amendment procedures are properly documented and controlled by management authorisation and subsequent review and
- physical and logical access to application data files are restricted and controlled.

Specific Control Issues

9.42 Most of the information systems we use today require networks and communication technology. Organisations, large and small from all over the world, are using networked systems and the Internet to locate suppliers and buyers, to negotiate contracts with them, and to service their trades. Uses of networks are multiplying for research, organisational coordination and control. Networked systems are fundamental to electronic commerce and electronic business.

9.43 End User computing practice is comparatively latest and while auditing it is an important consideration that data processed by end users on their own workstations is adequately controlled. End User computing is the ability of end users to design and implement their own information system, utilizing computer software products.

9.44 Also, a number of e-Governance projects are being launched by many governmental organisations for convenience of citizens while transacting with government bodies. A number of control issues have been thrown open by this new area of auditing. Such issues are outlined in the Chapter on e-Governance in Volume – II of the IT Audit Manual.

9.45 This section would focus on these specific control issues that cover the following:

- Network control and use of the Internet including the risk associated with networks and network controls.
- End user computing controls including risks associated with end user computing and the associated controls.
- IT Security

- Issues related to Outsourcing

Network and Internet Controls

Control Objective

9.46 The majority of systems encountered in medium to large scale organisations use either local or wide area networks to connect users. The use of networks is increasing and bringing organisations the following benefits:

- the ability to share data;
- to use and share other peripherals, e.g. printers;
- to leave system administration to a central team;
- allow users to send almost instantaneous messages, e.g. e-mail; and
- allow users to access the systems from remote locations.

9.47 Opening up systems and connecting them to networks is not without its risks. The network should be controlled such that only authorised users can gain access. Control of networks is not just about logical access security and keeping out hackers. Networks are primarily used to transmit data. When data is transmitted, it may be lost, corrupted or intercepted. There should be controls to reduce all these risks.

9.48 The scale of networks is also growing. Recent years have seen the growth of the Internet, the huge global network which allows millions of users to interact over communications links. The Internet has brought to light several issues which need to be addressed before deciding to connect up.

Risk Areas

9.49 Networks open up an organisation's computer systems to a wide, potentially anonymous user base. Where the organisation's systems are connected to networks, there is potentially a greater risk of unauthorised access by outsiders (hackers) and non-authorised employees, leading to:

data loss **- data may be intentionally deleted or lost in transmission;**

data corruption **- data can be corrupted by users or data errors can occur during transmission, e.g. a 1(in binary) is sent but due to interference, line noise etc, a 0 is received;**

fraud **- from internal and external sources;**

system unavailability **- network links and servers may be easily damaged. The loss of a hub can affect the processing ability of many users. Communications lines often extend beyond the boundaries of control of the organisation, e.g. the organisation may rely on the local telephone company for ISDN lines; wires may go through third party premises;**

disclosure of confidential information **- where confidential systems such as personnel, or research and development are connected to networks, there is an increased risk of unauthorised disclosure, both accidental and deliberate;**

virus and worm infections **- worm infections are specifically designed to spread over networks. Virus infections are very likely, unless traditional protective measures such as virus scanning are continuously updated. Users tend to scan disks they receive from external sources but are less likely to scan data received over a network; and**

contravention of copyright, **data protection (privacy) legislation, due to abuses by users of data or software available on the network or Internet.**

Audit Procedures

9.50 Because of the nature of networks, physical access controls are of limited value. The physical components of the network (wires, servers, communication devices) must be protected from abuses and theft. However, the organisation must place great emphasis on logical access and administrative controls.

9.51 The logical access controls will vary from one organisation to another depending upon the identified risks, the operating system, the network control software in use and the organisation's network and communications policies.

9.52 Before carrying out a review of the organisation's logical access and network controls, the auditor should review any technical material or publications on the organisation's systems. For example, if the IT auditor happens to have a copy of a publication on security and controls for the organisation's network operating system, he should review it before visiting the organisation's premises.

9.53 Controls which the auditor may encounter include:

network security policy**: this may be a part of the overall IT security policy;**

network standards, **procedures and operating instructions: these should be based on the network security policy and should be documented. Copies of the documentation should be available to relevant staff;**

network documentation**: the organisation should have copies of documentation describing the logical and physical layout of the network, e.g. network wiring diagrams for security reasons, these are usually treated as confidential;**

logical access controls**: these are especially important and the organisation should ensure that logons, passwords and resource access permissions are in place;**

restrictions on the use of external links **e.g. modems. These may be a weak link into the organisation's system, especially where the use of modems have not been approved;**

where the use of modems has been approved the organisation may have decided to use *call back modems*. These are modems which only allow access when they call out. For example a remote user at home wants access to the system. He uses his modem to call the office. The office system connects and asks for an ID code (and password), which the remote user enters. The office computer then disconnects. If the id code was correct the office computer dials backs on a pre-

programmed number, in this example the home phone number of the remote user. The auditor should note that call back modems are not foolproof as their controls can be bypassed by call forwarding and other technical attacks. There are other controls which use a token (an electronic device with a identification feature) to confirm that the external user has permission to access the system;

the *network should be controlled* and administered by staff with the appropriate training and experience. Those staff should be monitored by management;

certain *network events should be automatically logged* by the network operating system. The log should be periodically reviewed for unauthorised activities;

use of *network management and monitoring packages* and devices: there are many tools, utilities available to network administrators. They can be used to monitor network use and capacity. They can also be used to carry out inventory check on the software at each end user terminal;

***access by external consultants and suppliers* should be monitored. It may be the case that the organisation has allowed the software supplier a remote access link to carry out maintenance and bug fixes. The use of this facility should be monitored and access only given when required and approved. The modem should only be activated when approval is given by the organisation's management, and disconnected once the assignment is complete.**

***terminals may be restricted* to pre-defined terminals. This may be done via terminal codes, or ethernet (IP) address;**

***data encryption*: In certain circumstances the organisation may encrypt data on the network. Even if an unauthorised user could tap into the line and read the data, it would be encrypted and of no use.**

***use of private or dedicated lines*: If the lines are private and dedicated to network communications there is a lower risk of data interception. Dedicated lines are also normally able to carry more data and are less likely to result in data transmission errors they also cost more; and**

***use of digital rather than analog communication links*. Digital links tend to have a higher capacity; they don't require modems and do not suffer from digital to analog conversion errors.**

INTERNET CONTROLS

9.54 If you need to connect one of your computers directly to the Internet, then the safest policy is to:

physically isolate the machine from the main information system;

assign an experienced and trusted administrator to look after the Internet machine;

avoid anonymous access to the machine or, if it must be allowed, avoid setting up directories that can be both read and written to;

close all unnecessary logical ports on the Internet server;

monitor attempts to log in to the machine;

transfer files between the main information system and the Internet machine only when they have been carefully checked and remembering that programs can be transferred in the body of mail messages;

have as few user accounts as possible on the Internet machine and change their passwords regularly.

Firewall

9.55 Sometimes the business needs to connect directly to the Internet outweigh the risks. In such cases it is usual to construct a "firewall" to help control traffic between the corporate network and the Internet. Firewalls consist of a combination of intelligent routers and gateway hosts. A router can be set up to allow only specific Internet services between the gateway and other specified Internet hosts. Software on the gateway host may provide additional services such as logging, authentication and encryption, and packet filtering.

9.56 It is possible for an external computer on the Internet to pretend to be one of the computers on the corporate network. One particular function of the firewall is to stop any external packets that claim to be coming from the corporate network.

Internet Password Policy

9.57 Authentication is the process of proving a claimed identity. Passwords are one means of authenticating a user. It is fairly easy for an Internet user to disguise their identity and their location. Stronger forms of authentication based on encryption have been developed to reinforce the authentication process.

9.58 A good password policy can make a significant contribution to the security of computers attached to the Internet. All the password policies previously mentioned in this chapter are applicable to systems with Internet connections, e.g. on password ageing, sharing, composition etc.

9.59 If users must log in over the Internet then it pays to use a challenge and response system as previously described.

9.60 Every file on a computer connected to the Internet should have the minimum read, write and execute permissions consistent with the way that the file is used. Unix password files are particularly sensitive as hackers are likely to take copies for later analysis. Unix passwords are encrypted but there are readily available programs that will encrypt a list of words comparing each to entries in the password file. Since this can be done on the hackers own machine it will not trigger any alarms in the way that multiple unsuccessful attempts to log in should.

9.61 This attack is facilitated by the need for the etc/password file to be readable by everyone since it is read during the log in process. A partial defence is to use shadow password files and a modified login program. Using this approach the shadow password file can be protected whilst the etc/password file contains no real passwords. Another defence is to use a non-standard encryption algorithm.

Encryption

9.62 Two forms of encryption are widely used:

symmetric encryption uses the same key for encryption and decryption; and asymmetric encryption involves generating a pair of keys which are known as the public and private keys.

9.63 Symmetric encryption is fast but makes key distribution hard whereas asymmetric encryption is slow but does not suffer from the key distribution problems. A combination of the two approaches may provide the best solution.

10. AUDIT OF IT SECURITY and END USER COMPUTING CONTROLS

"Security in the end is your perception of the reality"

10.1 It is important that the organisation establishes an IT security policy which clearly states the organisation's position. The lower level, detailed controls should be based on the IT security policy. For example, detailed password controls would be based on the logical access section of the IT security policy.

Control Objective

10.2 By way of enunciating an IT security policy, the organisation:

- demonstrates its ability to reasonably protect all business critical information and related information processing assets from loss, damage or abuse;
- aims to enhance the trust and confidence between organisations, trading partners and external agencies as well as within the organisation;
- assure conformity to applicable contractual and regulatory requirements.

Risk Areas

10.3 Absence or existence of a weak IT security policy in an organisation may exclude the following basic principles of information security:

- Responsibility and accountability must be explicit
- Awareness of risks and security initiatives must be disseminated
- Security must be addressed taking into consideration both technological and non technological issues
- Security must be coordinated and integrated
- Security must be reassessed periodically
- Ethics must be promoted by respecting the rights and interests of others
- Security must be cost effective
- Security procedures must provide for monitoring and timely response

Audit Procedure

10.4 There should be specific statements in an IT security policy indicating minimum standards and compliance requirements for specific areas like (a) assets classification, (b) data security, (c) personal security, (d) physical, logical and environmental security, (e) communications security, (f) legal, regulatory and contractual requirements, (g) business continuity planning, (h) security awareness and training, (i) security breach detection and reporting requirements, (j) violation enforcement provisions, etc.

10.5 There are two basic level controls in an IT security policy – physical controls restrict individual physical access to IT resources and logical controls restrict access to specific systems to authorised individuals and to the functions each individual can perform on the system. It would be evident that many of the specific issues in IT security would be covered in this manual under coverage of various internal control objectives.

10.6 Nevertheless, the aspect of IT security is gaining ground and is being emphasised more frequently than before due to the strategic importance of data, reliance on data for decision making and confidentiality of data requirements.

10.7 IT security policies are normally expressed in the form of a concise narrative, i.e. a few pages of text. The policy requires senior management approval if it is to have any weight, and consequently should be approved at board level or equivalent. The policy should be seen to be backed by senior management. The policy should be available to all employees responsible for information security.

10.8 The organisation should also put in place methods for monitoring compliance with the policy and ensuring that the policy remains up to date.

10.9 It is also important that information security implementation in an IT application takes care of:

- Confidentiality of data meaning thereby that data or information is accessible only to those authorised to have access;
- Integrity, so as to safeguard the accuracy and completeness of information and processing methods; and
- Availability of data to authorised users and on time.

10.10 The objective of data security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity."

10.11 The concept of security applies to all information. Security relates to the protection of valuable assets against loss, disclosure, or damage. In this context, valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure. The protection is through a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics, firewalls, etc.

10.12 Many of the general and application controls are aligned with the above objectives of securing data as organisations may incur huge losses due to data loss. IT security involves implementing a suitable set of controls, including a secure environment, appropriate policies, procedures and practices, organizational structures etc. to address the specific security objectives of the organization. In addition to the risks associated with manual systems, IT systems are inherently open to certain additional risks. Some of the threats faced by IT systems are as follows:

- Fire
- Flood
- Power failure
- Earthquakes & other natural disasters
- Theft
- Intrusion and Hacking
- Technical failure
- Terrorist attacks

10.13 Consequently, Management needs to

- identify security risks and threats
- assess vulnerabilities of IT systems to such risks/ threats
- identify and select counter-measures, after due cost-benefit analysis,
- implement the counter-measures, and
- continuously monitor and review the risk environment and adequacy of counter-measures there against.

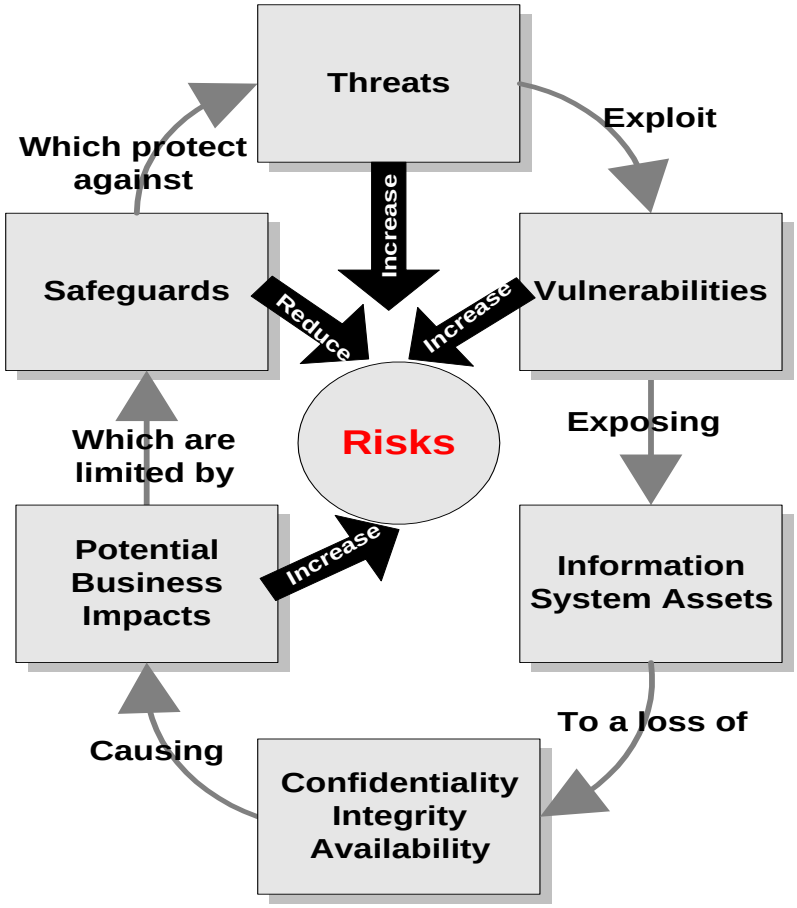
Risk Analysis

10.14 The extent of security measures required to be put in place depends on an assessment of risks and the perceived impact of these risks on business. The counter-measures would also depend on the extent of damage that these risks can pose to business and the estimated financial implication of such counter-measures. Risk analysis is not a one-time effort and needs to be carried out at periodic intervals in order to factor in changes taking place in technology, new threats emerging and the vulnerability of IT systems to such threats and the need to ensure that the current controls in place are working effectively.

10.15 Risk analysis involves:

- **business modelling** to determine which information systems support which business functions;
- **impact analysis** to determine the sensitivity of key business functions to a breach of confidentiality, integrity or availability;
- **dependency analysis** to determine points of access to information systems and assets that must be in place to deliver a service to a business function; and
- **threat and vulnerability analysis** to determine points of weakness in the system configuration and the likelihood of events that would exploit the weaknesses identified to cause impacts in terms of a breach of confidentiality, integrity or availability.

10.16 The following diagram illustrates the relationship between the various aspects of security that need to be considered in order to reduce the risk to an acceptable level:



10.17 An example of the output of risk analysis is depicted as follows:

Threat	Asset types	Disclosure / Confidentiality	Modification / Integrity	Destruction/ Availability
Fire, flood, hurricane, earthquake	Buildings, communication towers	Physical access controls may be abandoned during disaster recovery and discarded assets may hold confidential information		All services may be disrupted and data may be lost
Environmental failure including power loss	Hardware			Services will be lost and hardware may be damaged.
Theft	Valuable, portable assets	Stolen assets may hold confidential information		Services may be disrupted and data may be lost

Viruses	Software and Information		Data may be corrupted by viruses	Computers infected with viruses might crash or delete vital data.
Hacking	All networked systems	Surveys suggest that most attempts at unauthorised access are initiated by staff rather than outsiders but the trend towards connection to public information systems may alter this balance. The most common motivation for hacking is unauthorised disclosure of information but the hacker may decide to modify data or destroy it.		
Hidden code	All software and information	Unauthorised code may reveal sensitive information such as passwords	Hidden program functions may manipulate data.	Programs may be designed to destroy data or deny authorised access to services
Hardware failure	All hardware	Failed hardware may be discarded or sent for maintenance without purging sensitive information	Data may be corrupted when hardware fails	Denial of service
Software failure	Software and information		Data may be corrupted	Services will be unavailable
Personnel error	All systems	Staff may inadvertently disclose sensitive information by, for example, printing to the wrong printer	Staff may enter data incorrectly	Staff may destroy information accidentally, crash systems through configuration errors or damage hardware.

END USER COMPUTING CONTROLS

Control Objective

10.18 The term end user computing refers to the situation where users have intelligent computers on their desktops (i.e. computers with their own CPU processing capabilities), together with applications which allow them to develop their own processing, and reporting systems. End user computing has given users greater control over the processing and presentation of their data. Conversely, end user computing has reduced the control exercised by central IT departments.

Risk Areas

10.19 From the beginning, developments in end user computing environments have been uncontrolled. Users do not adopt the same standards or good practices that their colleagues in the IT department use. This uncontrolled environment can, and has led to a waste of time, effort and money for the organisation. The fact that end user computing has been so uncontrolled also causes the auditor concerns, especially where critical transactions are processed by end users.

10.20 The majority of end user computing problems and risks have arisen from the historical absence of controls. Users see their desktop computer as their territories over which they exercise their own controls and do what they like. This has led to several specific risks.

System Development

10.21 IT departments usually have staff experienced and trained in the development of computer systems. They are trained and have experience of:

- what standards the systems should be developed to;
- what documentation is required;
- what controls should be built into the new system; and
- what testing is necessary to ensure that the system does what it is supposed to do?

10.22 End user computing has permitted end users to develop their own applications without assistance from central IT departments. The end users developing their own systems do so without the relevant skills and training. When you have systems being developed in the absence of standards by non-experienced or trained staff, you invariably get problems. Typically these include:

unreliable systems which do not process data in the way intended, e.g. the underlying logic of the applications has not been thought through or coded correctly;

systems which do not include basic data integrity, input, processing or output controls. For example financial accounting systems which accept single sided double entries, resulting in unbalanced trial balances;

systems which are untested and unpredictable. For example, if the system has not been tested to ensure that it can deal with incorrect data input it may crash or hang when such data is entered by a user;

systems which are not documented. This makes it difficult to maintain the system in the longer term. IT auditors have frequently heard organisations tell them that an application was developed by an employee five years ago and since that person left no-one has been able to find any documentation to enable them to understand exactly how it works;

systems which have been subjected to uncontrolled change. End users have a habit of diving in whenever they find a problem in their own applications. They tend not to follow the same change control procedures as used in IT departments. This leads to changes which are poorly thought out and programmed. These changes may have a detrimental impact on the system. For example, a user may change a formula in a table, and unknown to him/her it has an unplanned knock on effect elsewhere;

incompatibility and fragmentation of information: the systems purchased by end users may be incompatible with the corporate systems. This makes on-line sharing of data difficult to achieve. Data on end user systems may not be up to date and include the latest amendments to the data on the central system.

Duplication of Effort

10.23 When end users take responsibility for their applications they tend not to consult with the rest of the organisation and rarely co-ordinate their efforts. This leads to duplication of effort as two different parts of an organisation attempt to develop an end user application to solve the same problem. Additional problems arise when they discover the duplication and nobody wants to shelve their project. Alternatively both may be developed, doubling the maintenance effort required to keep them up and running. As the systems were developed by different users it is possible that they produce different answers to the same problem.

Data Inconsistencies

10.24 Data may also be inconsistent from one user department to another. With traditional management and reporting hierarchies, updated information has to go up one branch of a management hierarchy before being disseminated back down another. Data inconsistencies are likely to be greater where the organisation uses a distributed system.

10.25 Data inconsistencies can cause the auditor problems if different parts of an organisation use different standing or master file data in their calculations, e.g. pay

rates for sub-contract staff, or unit costs for sales invoices or overhead apportionment rates for the calculation of full costs.

Increased Use of Resources and Costs

10.26 Experience has shown that end user computing has increased the cost of most organisations' IT services. The increased costs are not just from putting personal computers on users desks. Costs have increased due to increased training requirements, greater demands on help-desks. There are also additional hidden costs such as users spending more time trying to solve their own and their colleagues IT problems.

10.27 End user systems have a tendency to be less efficient in their use of resources, e.g. CPU time, networking and printing resources. For example, report writers require significant amounts of processing power, which can slow down the rest of a system. In some organisation users are not allowed to run their reports during normal working hours. Instead the reports have to be run overnight.

Erasure of Central Information

10.28 End users may download data from the central system for examination or processing with their own end user developed applications. Problems can arise where the flow of data is two way, i.e. after the user has processed the data it is then uploaded back into the central system, overwriting the original files. This increases the risk of information needed for audit being overwritten by incorrect information. In addition the audit trail may be obscured or lost when users overwrite the original data files.

Loss of Data

10.29 IT departments usually recognize the importance of regularly backing up data to ensure that if a problem or disaster occurs then the systems can be rebuilt, together with the data. Unfortunately, the same is not true in end user computing environments.

10.30 Another problem relating to the loss of data is the increase in computer theft. Computers, and especially the latest high tech personal computers, are valuable pieces of equipment. Their high value has made them targets of computer thieves. Whole computers may be stolen, together with the information they hold.

10.31 The increasing portability of end user computing in the form of laptop and notebooks has created a new risk. Their inherent portability increases the risk of a whole computer being lost or stolen e.g. when their computers are left on trains or stolen from hotel rooms, luggage racks or airports.

Access Security

10.32 A majority of personal computers use either DOS, Windows 95/98, Window 2000, Windows XP, OS/2 or Macintosh operating systems. These operating systems are designed for single users and consequently have little in the way of logical access controls to restrict access to unauthorised users.

10.33 It is reasonably easy to bypass any of the security controls which these operating systems use. Anyone with a reasonable knowledge of the operating system would be able to access any data file or application desired.

10.34 Physical access to desk-top computers is normally less controlled. An organisation's mainframe and minicomputers are usually located in a controlled environment with access restricted by locked doors, keypads combination locks and CCTV. The same is rarely true of end user computers. These are normally located on top of desks in the normal office environment.

10.35 Having physical access to a PC can be exploited to bypass the simpler logical access controls, e.g. the basic Windows type user passwords. Data may also be stored on floppy disks which can easily be copied. The data may also be edited or deleted by unauthorised users.

10.36 Where organisations make extensive use of end user computing, the auditor is likely to find that the general control environment will be weak. This may be due to insufficient staff to segregate duties, lack of training for computer users, inadequate resources or a lack of management commitment to establish standards and sound controls.

10.37 This inherent lack of general controls may increase the risk of errors and fraud. Where organisations use end user computing and the auditor is required to assess the possibility of relying on the computer controls, s (he) is more likely to look for the existence of management and administrative controls, rather than detailed technical controls within the computers and applications.

10.38 One of the biggest problems encountered by organisations when dealing with end user computing controls is ensuring that all the relevant staff is aware of the policies, standards and working practices that must be adopted. This may be overcome through a comprehensive education program for system users. Information can be passed through a combination of newsletters, bulletin boards and formal training.

Audit Procedure

System Development Controls

10.39 These may include establishing system development policies and standards for end user developed applications. The level of formalisation may be dependant upon the criticality of the application to the business. For example, where an application is important its development should be formalised and tightly controlled. On the other

hand where an application is not important and only used locally by a few employees, the development process would not have to be tightly controlled.

10.40 Development standards would ensure that the initial development of, and subsequent changes to, important applications are subject to approval, and that they are documented and adequately tested.

10.41 The problems associated with incompatible systems can be reduced if the organisation has policies and procedures for the acquisition of hardware and software. The policies may also include procedures for making asset purchases and recording asset locations in a register.

Duplication of Effort

10.42 Users should have a mechanism by which they can communicate their efforts to others in an organisation. This could be done by arranging regular meetings between middle and lower level management. Local developments in IT systems could be one of the discussion items on the agenda.

Data Inconsistencies

10.43 Where updated information is important, the organisation should have a system to ensure that all those using the data have an up to date copy. This problem is normally solved by holding the data on a central database. The applications developed by end users could use the information in the database instead of relying on outdated information in local data files.

10.44 The organisation could also have procedural controls to ensure that the most up to date information is used. For example a check list could be drawn up to prompt users into using the latest information.

Where users can access the information contained in a central database, access permission should be established so that only authorised users can amend the central data.

Legislation

10.45 The organisation should establish policies to ensure that end users are aware of, and comply with relevant legislation. The awareness program may cover:

software theft: i.e. the unauthorised copying of an organisation's software or data for personal use or gain;

compliance with health and safety legislation;

the use of pirated and illegal software; and

the collection, use and storage of personal information (privacy legislation).

Data Loss

10.46 Where important applications or data are stored on end user computers, the organisation should establish controls to ensure that the organisation would not be adversely affected by a disaster affecting those computers.

10.47 Control procedures could include:

requiring users to back up their applications, data and documentation on a regular basis and storing the back-ups in a secure location (off-site if required). The frequency of backups should be dependant upon how important the data is, the timeliness of the data and how many transactions are processed in a given period; and

storing data on a fileserver instead of on local hard or floppy disks. The fileservers are normally administered by the IT department and should have established procedures for backing up the data on a regular basis.

Logical and Physical Access

10.48 Users should be encouraged to adopt at least basic logical access security precautions on their standalone personal computer, e.g. setting the BIOS password. If possible, data should be stored on network fileserver. In general the network operating system will provide a degree of protection against unauthorised access via the network.

10.49 Where an organisation uses portable computers, there should be policies which require them to be placed in a secure environment overnight, e.g. in a locked drawer or cupboard. Even organisations with 24 hour security have experienced lost or stolen laptop computers.

10.50 Where the organisation considers risks to be particularly high consideration should be given to installing security software on end user computers. These should have more robust logical access controls and may encrypt sensitive data.

End User Support

10.51 End user computing is on the increase and is likely to become more significant in the future. The organisation should have established a framework to provide users with support.

10.52 End user support is normally provided via a help-desk function. The help-desk acts as the interface between the IT professionals in the IT department and the end users. User request for help should be passed on to the IT specialist with the appropriate skill and knowledge.

Protection against Computer Viruses

10.53 There are a number of controls that an organisation could put in place to reduce the risk of viral infection. Some are technical in nature other are administrative and procedural. Staff should be made aware of the risks and informed of the measures adopted by the organisation to manage the risk.

Use of Anti-virus Software

10.54 There are many products in the market which claim to detect computer viruses. The software should be supported by a screening policy. The policy should require all incoming media to be scanned for viruses before it is loaded onto a computer.

10.55 Anti-virus software may be installed on every computer or alternatively one could be set up as a standalone “sheep-dip” computer. Ideally the anti-virus software should be as transparent to the users as possible, i.e. it should be unobtrusive.

10.56 Some anti-virus software only scans when prompted by the user. Others provide continuous protection by loading a TSR (terminate and stay resident) program into memory. TSR anti-virus programs keep a constant lookout for viruses and run as a background program.

10.57 However, the anti-virus software runs the risk of always being one step behind the virus writers. Even where anti-virus software is used there may be a new virus which the software cannot detect. This makes regular updating of the virus scanners very important.

Back-ups

10.58 It is very important that users regularly back up their computer files. Back-ups can be made less onerous by using automatic backup software.

11. USING COMPUTER ASSISTED AUDIT TECHNIQUES

Introduction

11.1 Once the auditor completes the evaluation of internal controls, it is necessary to plan for obtaining sufficient, reliable and relevant evidence to support his/her conclusions on the effectiveness of controls. The auditor also needs to obtain assurance that the data processed by the system is complete, valid, and accurate and is giving the desired results. This is where CAATs come in handy.

11.2 CAATs can also be used as a starting point by way of Reverse Flow Technique to generate exceptions and then zero in on the deficiencies in controls environments. This is explained below in para 11.5

What are CAATs?

11.3 Computer Assisted Audit Techniques (CAATs) are computer based tools, which help an Auditor in carrying out various automated tests to evaluate an IT system or data. These are very useful, where a significant volume of auditee data is available in electronic format. CAATs provide greater level of assurance as compared to other techniques, especially manual testing methods, due to the following reasons:

- Key account areas can be analysed in-depth
- Large volumes of data can be tested and analysed 100% within a short span of time and with less effort
- Tests can be repeated easily on different files/data
- Tests can also be flexible and more complex with change in parameters
- Documentation of audit tests and results can be generated by these tools
- Scarce audit resources can be deployed more efficiently and effectively

Role of CAATs

11.4 With a significant number of auditee organizations computerizing the core areas of their operations, CAATs are being increasingly used by auditors for substantive and compliance testing, both in Financial and Compliance audits and Performance audits including forensic audits. The audit objectives remain the same even with the use of CAATs. However, the audit methodology will be different, since audit trail and evidence will be invisible in most cases.

Use of CAATs and the extent of usage are determined by various factors during audit planning and execution stages as detailed below.

Audit Planning Stage

11.5 At the audit planning stage, the thrust is on audit effectiveness:

- Auditors can use CAATs to run through the data and carry out initial trend analysis and summarize the data by key fields so as to identify the focus areas and unusual items for detailed in-depth examination.
- Auditors can also play around with the data and identify unusual items and exceptions, which could help in planning for performance and forensic audits.

Audit Execution Stage

11.6 At the audit execution stage, the focus is on efficiency:

- At this stage, the auditors will be able to use CAATs to interrogate the data/files extensively by applying various parameters.
- Appropriate samples can be generated by using statistical sampling methods (in-built in certain CAATs software).
- The quality of data can be ascertained by analyzing the gaps, duplicates and missing records
- There can be savings in time, cost and manpower.

Types of CAATs

11.7 There are two types of CAATs – those that are used for scrutinising and ***validating the programme*** and those that are used for analyzing and ***verifying the data***. Generally, programme analysis requires a higher level of expertise on the part of auditors than data analysis. The auditor needs to have technical knowledge and skills related to the specific architecture and environment of the auditee's IT system. Considering the availability of limited staff trained in advanced IT audits, it may not always be feasible for the SAIs to carry out programme analysis.

11.8 Data analysis on the other hand, generally ignores the programmes that generate the data and focus more on validating the data that is processed by the system. In the process, the control environment can be assessed quite effectively, which in any case is one of the important reasons for carrying out programme analysis.

11.9 Programme analysis is used basically for compliance audits while data analysis can be used for performance and forensic audits apart from compliance audits.

11.10 This method is used basically to identify redundant code or code used for fraudulent purposes. This is done by executing the programme to see if any unauthorized changes have been made to the software.

User Log Analysis

11.11 Almost all the systems maintain logs of user entries like log on and log off. Such logs are available as text files or part of the database in many systems. Analysis of these logs will enable the auditor to identify unauthorized entry of users and failed attempts to log into the system and investigate further into these cases.

Data Analysis

11.12 Data analysis is the most widely used form of CAATs and a number of tools and audit software programmes are available in the market for the purpose. These data analysis tools are generally suitable for PCs and can be used for any type of audit *viz*., performance audit, financial audit, compliance audit and forensic audit. Some of the important functions performed by auditors using data analysis tools are detailed below:

Exception Reporting

11.13 The auditor can extract data fulfilling or violating certain specified criteria, or cases which are exceptions from the given data, for further detailed study. For instance, the auditor may want to identify all cases of purchases above Rs. 1 lakh or all the employees who have been recruited during the last five years. These and similar exceptions can be extracted easily by the auditor using data analysis software.

Totalling

11.14 Totalling can be done by the Auditor to check the completeness of the data and the figures given therein. This is also done to reconcile the given account.

File Comparison

11.15 This is done to check the data changes from one month to another or from one period to another and to identify the changes that have taken place during this period.

Stratification

11.16 This provides the auditor with a full range of values within the file so that he/she can analyse the data more in-depth and also group the data for sampling the transactions in a systematic and intelligent manner.

Sampling

11.17 The Auditor can pick out samples which represent the entire population in a scientific manner by using any of the sampling methods provided within the audit software.

Duplicate Checks

11.18 Data analysis software facilitates identification and analysis of duplicates in a given file. For instance, it is easy to identify duplicate invoices, users, payments, items, etc. This could help in not only evaluating input controls in the system but also in detecting fraudulent transactions.

Gap Detection

11.19 This facility in audit software will enable the Auditor to identify the gaps in the data like invoice numbers, dates, purchase orders, etc. which could indicate once again lack of controls within the system and possible frauds.

Ageing

11.20 The auditor can group transactions by their age to see if the organization's procedures are working properly. For instance, it is easy to see the time taken from issuing a purchase order to the receipt of goods and the release of payment for the same. Also, the Auditor can analyse the debtors and creditors extensively through this means.

Analytical Audit Procedures

11.21 CAATs can be used by the auditor to carry out analytical audit procedures like trend analysis, ratio analysis, proportional analysis, benchmarking and modelling techniques, which can facilitate a comparison of inter-relationships among various sets of data and highlight areas of audit concern.

Data Mining

11.22 This refers to mining or extracting important information from vast amounts of data and is used primarily with regard to decision support systems, which provide enormous amount of data. Here the auditor can dig deep into the data and spot the trends and patterns over a period of time which would help in identifying unusual transactions for detailed study. This is very useful while carrying out performance or forensic audits.

Calculations

11.23 Calculations can be performed to ascertain the accuracy of the formulae used by the auditee. Also, the input data can be reprocessed to validate the controls and compare the results of such reprocessing with the data provided by the auditee from the system.

Virtual Fields

11.24 CAATs can be used to create additional fields in the auditee data so as to extract records fulfilling certain criteria or to create calculated fields by using the auditee's data.

Other Data Analysis Functions

11.25 Other than the functions mentioned above, CAATs can also facilitate sorting of data in a file, summarising, casting, recomputing and recreation of audit trail.

Determinants of CAATs Choice

11.26 There are a few factors that need to be considered by the audit teams while deciding on the use of CAATs. These are detailed below:

- Does the use of CAATs provide additional value to audit?
- Are the tests going to be repeated in other/future audits of the same auditee or other auditees whose nature of business and operations are similar?
- Is the area under review a high risk/high priority area?
- Is it a business critical system?
- Are the transactions processed on-line and/or real-time?
- Will the use of other audit techniques entail higher costs and extra time?

11.27 Normally, CAATs are used for ***programme analysis*** when the application is mission critical and where data analysis cannot be relied upon to provide assurance as to the adequacy and effectiveness of controls.

11.28 CAATs are used for ***data analysis*** where the auditor needs to repeat the tests for future audits. Also data analysis tools are useful while auditing online and real time transaction processing systems and other high risk systems.

Data Analysis Tools

11.29 Numerous tools are available for data analysis purposes. Some of these are–

- General purpose audit software
- SQL and SQL based tools
- Microsoft Access and
- Other tools like Microsoft Excel

General Purpose Audit Software

11.30 These are ready-built audit software available off-the-shelf. These are developed to meet the specific requirements of auditors, and contain all the regular tests that are carried out by auditors as part of IT audit and include common functions like data extraction, summarizing, aging, stratification, duplicate checks etc. Common examples of general purpose audit software

include IDEA (Interactive Data Extraction & Analysis), and ACL (Audit Command Language). Both these packages are MS Windows based and are capable of importing data from and exporting data to a wide variety of formats.

11.31 IDEA is quite user friendly and is being used in IAAD for the past many years for data analysis purposes. The Windows version of IDEA especially, offers all the common Windows functionality including ODBC drivers provided by Windows, to help the auditor in importing files/data from a wide range of file formats.

11.32 Another audit tool is 'Applaud', which is a good data analysis software but takes up a lot of memory. It is also not very flexible in terms of importing data from different file formats. The other generalised audit software available include 'Prospector', 'Sage Sterling' and 'CA Panaudit Plus', which are all capable of performing data extraction and analysis functions.

SQL Tools

11.33 SQL (Structured Query Language) is a non-procedure oriented language and does not require advanced programming skills to run queries. SQL is used for defining and manipulating data in Relational Database Management Systems (RDBMS) and the SQL standard formulated by American National Standards Institute (ANSI) and International Organization for Standardization (ISO) are followed by all the RDBMS products. This makes it easy for auditors to run queries on databases and platforms of which they are not very conversant.

11.34 The SQL based tools available in Microsoft products in fact, provide user friendly interface for selecting the required data and specifying the criteria for data extraction. This would enable the auditors to run queries directly on the auditee databases, in case he/she has problem downloading the data onto the desktop. Alternatively, the auditor can download the data onto his/her PC/Note Book and interrogate the data using SQL. However, SQL is not effective to use on legacy systems and despite its simple syntax, it is also not very advantageous to an auditor who does not possess appropriate programming skills. This is due to the fact that unlike the others generalized audit software, the audit routines like data extraction, summarizing etc. are not built into the SQL tools.

11.35 While most auditee organizations are averse to granting access to auditors to their systems/databases, it is also not advisable for auditors to use SQL to run queries on the auditee database directly due to the following reasons:

- the performance of the system could be adversely affected, in case complex queries are run
- the auditor could inadvertently modify or delete the data in the auditee system

- the auditor may not be able to safeguard his/her work and the audit evidence may be tampered with if the data analysis is carried on the auditee system

Microsoft Access

11.36 Microsoft Access is a part of MS Office suite of products and is a good desktop based database. It can be of great help to the auditors in running queries and for importing/exporting data from / to a variety of formats. It is also easy to import data from other RDBMSs like Oracle, etc. The constraint of course is the fact that each of the Access databases cannot exceed 2 GB and the performance is affected, in case the queries result in the creation of larger files.

Other Tools

11.37 Spreadsheets are also useful for CAATs purposes. Packages like Microsoft Excel can be used for running simple queries like extracting data fulfilling certain criteria, sorting, totalling etc. However, the number of records in a single file can pose problems while using software packages MS Excel for data analysis purposes.

11.38 Another tool available for data mining purposes is WizRule (from WizSoft Suite), which can run through large quantities of data and generate hundreds of possible hypotheses/rules. It can access databases like Oracle and Access and can function like an on-line analytical processing (OLAP) tool.

Data analysis Tools in IAAD

11.39 Within IAAD, we use a number of data analysis tools like IDEA, MS Access, Excel, SQL and ACL (to some extent).

- IDEA is quite user friendly and has most of the normal audit tests built-in. ACL also features most of the audit tests. However, both these products require specific licenses which are expensive.
- Microsoft Office products on the other hand, are much cheaper and every Office in IAAD has enough licensed copies of these.
- MS Access is quite powerful while linking tables and setting relationships with regard to data imported from RDBMSs. The querying functions of Access are also very flexible.
- SQL is again a very effective querying tool but as mentioned earlier, it has certain limitations due to the absence of in-built audit functions.
- Spreadsheets can be used effectively for simple data analysis and graphical representation of audit results obtained through MS Access.

Data Analysis Using IDEA

11.40 The current IDEA version in use in IAAD is IDEA 2002 (educational version of IDEA 2004 is available). The ‘Help’ function in IDEA 2002 is quite exhaustive and gives step-by-step directions about the mode of running various

queries. Apart from giving the details of queries, the IDEA 2002 'Help' function also gives tips relating to the possible audit tests / analysis that can be done in different areas and circumstances. It also provides an overview of functions of different systems and possible fraud scenarios. As the Training Module of IAAD on IDEA covers the various aspects of using the same except downloading ORACLE Data in to IDEA (Explained later) this Manual is not going into the details of running queries in IDEA.

Data Analysis Using MS Access

11.41 There are five types of queries that can be run in MS Access viz.

- Select queries
- Parameter queries
- Cross-tab queries
- Action queries
- SQL queries

11.42 MS Access can use multiple tables in queries and can set up complex relationships between tables to enable the auditors to retrieve data to their specifications. It can also join and set relationships between copies of the same table (**self-join**) or query, to produce certain advanced queries.

11.43 **Grouping / summing / totalling** function is another very convenient tool in the Queries module of MS Access. It can give the minimum / maximum / average value of a field. It can **count**, and can also provide **expressions**, **standard deviation**, **first** and **last record** and the '**where**' expression.

11.44 Some sample queries are given in **Volume II** detailing how to analyse the VLC Data using MS Access.

10.45 When queries are run in MS Access, it constructs equivalent ***SQL statements*** behind the scenes. The auditor can view or edit the statements in SQL view. For some SQL queries which are called **SQL – specific queries**, SQL statements should be created directly in the **SQL view** rather than by using the **Design view**.

Data Analysis Using SQL

11.46 The main SQL statement used by the auditor (and often the only one!) is the **SELECT** statement. An example of a simple SQL SELECT statement is as follows:

SELECT Empno, Name, Joining_Date FROM EMPLOYEE_MASTER WHERE Dt_of_birth < #01/01/1980#

11.47 The above statement can be broken up into the following parts:

- The EMPLOYEE_MASTER table from which the data is being 'selected', which is specified using the '**FROM**' clause;

- The fields Empno, Name, Joining_Date in the EMPLOYEE_MASTER table, which are of interest to the auditor; and
- The condition that only data records where the field Dt_of_birth is less than 01-01-1980 need to be selected, which is specified using the '**WHERE**' clause.

11.48 Every SQL query of interest to the auditor will be modelled on the same pattern. However, there are a number of options and clauses that can be used by the auditor to prepare sophisticated and complex queries, which are fine-tuned to his requirements as described later in this Chapter.

Tip 1: The best way for an auditor to learn the different nuances of the SELECT Statement is to carefully study the SQL Syntax of the queries designed in MS Access using the Graphical interface.

Tip 2: There is no substitute for experience. Each CAATs audit teaches a few tricks to the auditor for a particular purpose, which will invariably be useful in a different context in the future.

How to Use CAATs?

11.49 Having decided to use CAATs to audit a particular area, the auditor should plan how exactly he/she is going to do that. It is important to get the correct data and get it correctly. It is therefore imperative to understand the following aspects thoroughly:

- The auditee organization and its operations;
- The IT systems under review;
- Working of the IT system-
  - the structure of the database;
  - the details of the files / tables;
  - data dictionary
  - the relationship between the files / tables;
  - the database triggers;
  - users of the systems;
  - input / output data;
  - reports generated by the systems and so on.

11.50 The auditor should then document his / her understanding of the system and have it confirmed by the auditee organization. Determine the tests that are to be performed on the area / system under review and identify all the related files / tables to be analysed.

Data Downloading

11.51 That brings us to the question - how do we transfer / download the identified data from the auditee's IT system on to our desktop/notebook in a suitable format to enable us to analyse it using CAATs? Here the auditor needs to understand the data structure and the file formats.

Data Storage

11.52 Data is stored in computers in binary mode, which uses only 2 symbols (0 and 1) unlike decimal system, which uses 10 digits (0-9). While data is stored in binary form, it is represented in hexadecimal form, which has a base of 16 values (0-9 and A-F). Since the most common unit of computer data is the byte, hex can represent all the bits in a byte using just 2 hex digits, each one representing four of the byte's eight bits.

File Formats

11.53 There are many applications however, which use data as text. These applications use some form of code to represent binary numbers as text for display purposes. The commonly used such codes are ASCII (American Standard Code for Information Interchange), EBCDIC (Extended Binary Coded Decimal Interchange Code) and Unicode. While ASCII is used in many of the mini and micro-computers, in most of the mainframe systems, data is stored in EBCDIC format. Each of these formats uses different series of decimal values to represent letters, numbers and control characters. With Windows NT, Unicode format is being used by the desktops world over. Unicode encoding supports almost all the major world languages and displays text in two languages – English and one foreign language.

11.54 Data can be stored in computers in various forms such as,

- Flat file systems
- Relational Database Management Systems (RDBMS)
- Other forms

Flat Files

11.55 In flat file systems data is stored as a simple text file like ASCII or EBCDIC, which can be viewed directly using a text editor. These formats are written in 'High Level Languages' like Cobol, Fortran etc. and were basically used in legacy systems, most of which were migrated to RDBMS later on.

11.56 Normally, in flat file systems there are a number of data files, each of which contain several data elements with no inherent relationships between the files. Relationships have to be created using programmes. This leads to redundant data and could pose problems in terms of data integrity. This also results in wastage of storage space.

11.57 Flat files can be categorized further into the following:

- Fixed length data
- Variable length data
- Delimited data

11.58 As mentioned earlier, most of the legacy systems use flat files. A number of generalised audit software provide facilities for downloading and converting data from flat file systems into a format which can be used by the auditor for analysing the data. However, it is a tedious and time consuming process.

Relational Database Management Systems

11.59 These days most of the IT systems use the relational database model for storage of data. Here the data is stored in a normalised fashion in the form of inter-related tables which would automatically reduce redundancy of data as well as storage space. RDBMSs also use primary and foreign keys to uniquely identify the records and their values in a table with a related table. In a RDBMS, queries are built using SQL, which is also used for data definition and data manipulation. RDBMSs also offer very good security features.

11.60 Relational database products are offered by numerous vendors like Oracle, IBM, Microsoft, Sybase, Informix, Ingress etc. The most popular and widely used relational database is Oracle. In order to download data from a RDBMS, the auditor needs to have a good knowledge of the concepts of relational databases.

Other Forms

11.61 Among the other forms of structured data storage is Microsoft Access, which is more or less a relational database without the client server networking, and security features of a RDBMS.

11.62 Another form of structured data storage is an ERP (Enterprise Resource Planning) System which is being widely used by many organizations across the world for integrating the functionality offered by various systems. These ERP Systems use a relational database as data storage and also include many audit related features for querying the database. Some of the audit tools like ACL provide direct link to ERP Systems like SAP.

11.63 The IT audit guides prepared by IAAD earlier, as well as the guides and training courseware prepared by the INTOSAI IT Audit Committee had given detailed write-up about the different formats of data and the mode of conversion and downloading of such data into the auditor's desktop. We will not go into these details again in this document.

11.64 In a survey conducted by the IAAD on the usage of the different platforms and databases by the auditee organizations, it was revealed that a majority of the auditee systems use Oracle database followed by FoxPro, MS Access, dBase, SQL Server. Since data from all the systems using these databases can be downloaded either directly or through ODBC (Open Database Connectivity) drivers, we will discuss this mode of data downloading here. ODBC is a standard method of sharing data between databases and

programmes and the ODBC drivers use the standard SQL to access external data.

Pre-requisites for Data Downloading

11.65 For downloading data from any system, the auditor has to obtain written permission from the auditee management. The IT Department of the auditee / the database administrator (DBA) has to set up the auditor as a user in the system with specific permission to access the required and authorized data for 'read-only' purposes.

11.66 Data can be downloaded through any of the following methods:

- Using any of the storage media like CD-ROM, USB Drive, Floppy, DAT Drive, Magnetic Tape Drive, Cartridge Tape Drive etc.
- By plugging into the auditee's internal network (of course, with the permission of the auditee Management/IT Department) and setting up an ODBC connectivity
- Through e-mail from the auditee, depending on the speed of the internet connectivity. (Leased lines / dedicated lines offer better facilities for large volume of data transfer rather than dial-up connection).

11.67 Irrespective of the mode of downloading auditee data, the auditor needs to obtain the following information/details from the auditee:

- Details of files / tables – Master tables and transaction tables
- Relationships between the files / tables (if it is RDBMS)
- Database triggers
- Data dictionary
- Record layout (the name, description, length, type and decimal places of all the fields in the record)
- Number of records in each file / table
- Size of the file / table
- Format in which data is given (if it is a flat file)
- Medium for data transfer
- Any associated file and logical relationship if any, between the fields of associated files
- Control totals
- Details of header, trailer blocks, number of blocks, number of bytes in each block and the blocking factor if the data is provided in magnetic tapes
- System and data documentation including documentation updates.

Annexure

IT CONTROL FRAMEWORKS

Since the 1980s the IT community has seen a number of Standards and Control frameworks. The prominent ones amongst them are CoBIT, CMM, SAC, ISO, ITIL, BS7799 etc. These were a result of deliberations which came out of various reports such as COSO, CoCo, Cadbury, Kings Commission etc. The most widely accepted and advanced information security standards and IT frameworks that exist today are described below in brief.

1. CoBIT

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 organisational 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 Organisation, 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:

- **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 realisation of the strategic vision need to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure must be put in place.
- **Acquisition and Implementation**: To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and 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.
- **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.
- **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 organisation'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 organisation is today, where it

stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; **Critical Success Factors**, which define the most important management oriented implementation guidelines to achieve control over and 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.

Key Points: Introduction of CoBIT in IA&AD for IT Auditing

- 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 goes on to provide a generic audit guidelines template to assist in the evaluation and testing of the control objectives, The generic approach is to obtain understanding of the process, evaluate controls, assess compliance, and substantiate the risk of control objectives not being met. The template is applied to each of the 34 processes, with specific audit guidelines detailed within each process.
- CoBIT is a way of thinking. Successful adoption requires orientation, education and training.
- CoBIT is a framework that can be tailored according to the IT environment of the auditee organisation and risk assessment.
- CoBIT is not a collection of IT controls and audit programs. CoBIT contains IT control objectives that generally must be addressed by most auditee organisations and audit guidelines that may be used to assess performance against those IT control objectives.
- CoBIT is an example of clear policy and good practices for IT control and audit that can be used to guide audits.
- Also CoBIT framework can be used for performing risk assessments and to guide the development of individual IT audit plans.
- The IT Audit programs can be tailored to include activities from CoBIT audit guidelines.
- Compliance focused audit entities and those with less than warm relations with the auditee organisations may need to depend on a mandate for adoption of the CoBIT framework.

- **In IAAD CoBIT is now ingrained in the processes with most of the audits borrowing heavily from the audit guidelines of CoBIT. Moreover multiple audits have been undertaken, and are being conducted using CoBIT as a framework**.

2. Capability Maturity Model

The CMM Model is briefly described below:

(i) Capability Maturity Model Software Acquisition (CMM SA)

The Software Engineering Institute's (SEI), at Carnegie Mellon University, "Software Acquisition Capability Maturity Model" (SA-CMM) enables an audit agency to quickly assess the maturity of an agency's software acquisition process. The results of such an audit can serve as a roadmap for process improvement. The SA-CMM ranks organizational maturity according to five levels.

At Level 1, the software acquisition process is characterized as being adhoc, and occasionally even chaotic. Few processes are defined and success depends mainly on the individual efforts of program managers and staff. Success cannot be repeated consistently because staff members take their skill with them and groups have little to rely on when key members leave or are assigned to other projects.

At Level 2, basic project management processes are established to track performance, cost, and schedule. The necessary process discipline is in place to repeat earlier successes on similar projects.

Levels 3 and 4 build on project management processes and provide a standardized and established set of software acquisition process for the entire organization (or groups). Projects use an approved, tailored version of the organization's standard software acquisition process if necessary, and measures of quality of the software acquisition processes, products, and services are collected.

At Level 5, continuous process improvement is empowered by quantitative feedback from the process and from piloting innovative ideas and technologies.

(ii) CMM (Software)

- Capability Maturity Model for Software (SW-CMM) is a framework that describes the key elements of an effective software process. The

CMM describes an evolutionary improvement path from ad hoc, immature process to a mature disciplined process.

- The objective behind the framework was to provide a model that is based on actual practices, reflects the best of the state of the practice, reflects the need of the individual performing software process improvement and **software process assessments**, is documented and is publicly available.
- The need for such best practices was felt because of reliance on software intensive systems to perform core missions. CMM is a logical framework for base lining an organisations' current process capabilities (i.e. strengths and weaknesses)
- **Definition:** CMM is an ordered collection of practices (processes) for the acquisition, development or maintenance of (software – intensive) systems. It is ordered by Key Process Areas.
- It defines the stages through which organisations evolve as they improve their acquisition and implementation processes. It also identifies key priorities, goals and activities on the road to improving an organisations' capability to do its job. It is intended to be independent of the application domain and any specific technology. It also applies to the acquisition of in-house software development
- **Why focus on process?**
  Everyone realises the importance of having a motivated, quality work force, but even our finest people can't perform at their best when the process is not understood or operating at its best.
- **Maturity levels**
  A maturity level is a well defined evolutionary plateau on the path to becoming a mature software acquisition / development organisation.
  There are five maturity levels in CMM.
  Maturity levels may not be skipped. Each level is a layer in the foundation for continuous process improvement.
- **Key Process Areas**
  Key Process Areas (KPA) are a cluster of related practices performed collectively to achieve a set of goals. Each maturity level in CMM is composed of several Key Process Areas.
  They are the major building blocks in establishing the process capability of an organisation.
  Each KPA has been defined to reside at a given maturity level.
  There are 16 KPA in the CMM (SW).
- CMM can be adopted in IT Auditing for software process assessments, in which a trained team of IT Auditors determine the state of the organisations' current software process and reports the high priority software process related issues facing an organisation.

(iii)Capability Maturity Model People (People CMM)

The People Capability Maturity Model (People CMM) is a framework that helps organizations successfully address their critical people issues. Based on the best current practices in fields such as human resources, knowledge management, and organizational development, the People CMM guides organizations in improving their processes for managing and developing their workforces. The People CMM helps organizations characterize the maturity of their workforce practices, establish a program of continuous workforce development, set priorities for improvement actions, integrate workforce development with process improvement, and establish a culture of excellence. The People CMM consists of five maturity levels that establish successive foundations for continuously improving individual competencies, developing effective teams, motivating improved performance, and shaping the workforce the organization needs to accomplish its future business plans. Each maturity level is a well-defined evolutionary plateau that institutionalizes new capabilities for developing the organization's workforce. By following the maturity framework, an organization can avoid introducing workforce practices that its employees are unprepared to implement effectively. Moreover, once executives identify an organization's strategic objectives, the People CMM provides guidance that improves the organization's ability to satisfy those objectives through a competent, capable workforce.

3. 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

4. CoCo

The formal name of this report is Guidance on Control. It was published by the Criteria of Control Board (CoCo) of the Canadian Institute of Chartered Accountants (CICA) in November 1995. CoCo defines control and specifies criteria for effective control. The CoCo control framework is intended to be used by people throughout an organisation to develop, assess, and change control.

CoCo defines control as "those elements of an organisation (including its resources, systems, processes, culture, structure and tasks) that, taken together, support people in the achievement of the organisation's objectives." It defines three categories of objectives:

- Effectiveness and efficiency of operations;
- Reliability of internal and external reporting;
- Compliance with applicable laws and regulations and internal policies.

5. Cadbury

The formal name of this report is Internal Control and Financial Reporting. It was published in December 1994 by the Committee of the Financial Aspects of Corporate Governance (Cadbury Committee) of the Institute of Chartered Accountants in England and Wales (ICAEW).

Cadbury** initially defines internal control as**:

The whole system of controls, financial and otherwise, established in order to provide reasonable assurance of:

- effective and efficient operations
- internal financial control
- compliance with laws and regulations

The internal controls are established in order to provide reasonable assurance of:

- the safeguarding of assets against unauthorised use; and
- the maintenance of proper accounting records and the reliability of financial information used within the business or for publication."

Cadbury requires that the board of directors of every company incorporated in the United Kingdom publish a statement about their system of internal financial control. The statement must, at a minimum, acknowledge the following:

- The directors are responsible for internal financial control
- An explanation that the system can provide only reasonable, not absolute assurance against material misstatement or loss

- A description of key procedures that the directors have established to help ensure effective internal financial control
- Confirmation that the directors have reviewed the effectiveness of the system of internal financial control

It encourages directors to state their opinion on the effectiveness of the system of internal financial control.

The criteria for assessing the effectiveness of internal financial control in Cadbury fall into the following five categories:

- Control environment
- Identification and evaluation of risks and control objectives
- Information and communication
- Control procedures
- Monitoring and corrective action

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.

Apart from the IT guidelines, International Standard on Auditing published by IFAC contains International Auditing Standard 400 for Risk Assessment and Control and International Auditing Standard 401 on Auditing in a Computerised Information System environment. Also International Auditing Practice statements No. 1001, 1002 and 1003 deal with auditing issues related with IT environments for Stand Alone computers, online systems and database systems respectively.

7. British Standard 7799-1:2000

BS7799 is the British standard for Information Security Management. It has now become an International Standard, ISO 17799. It is in two parts - Part 1

sets out approximately 40 objectives for Information Security, and Part 2 has about 130 controls which can be implemented to achieve those objectives.

It is applicable to every organisation, whatever the type of organisation, and whatever its size. There are a rapidly-growing number of organisations who not only comply with it, but also are independently certified to be complying with it. There are both British and International Users' groups. It provides organisations with a framework of Information Security, which can be recognised by other organisations.

BS7799 is the most widely recognised security standard in the world. Although it was originally published in the mid-nineties, it was the re-vision of May 1999 which really put it on to the world stage. Ultimately, it evolved into BS EN ISO17799 in December 2000.

BS 7799 (ISO17799) is comprehensive in its coverage of security issues, containing a significant number of control requirements. Compliance with it is consequently a far from trivial task, even for the most security conscious of organisations.

8. SAC Report of Institute of Internal Auditors

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.

9. ITIL

The methodology of ITIL (IT Infrastructure Library) was developed by experts of CCTA (Central Computing and Telecommunications Agency) for the purpose of supporting high quality and cost-efficient IT services. Sponsored by UK Office of Government Commerce, ITIL determines the implementation of service management functions in their whole life-cycle: design, introduction, operation and introduction of newer services. ITIL is a consistent and comprehensive set of documents containing procedures and best practices accepted in the IT industry in the field of IT service management. However it doesn't address the development of quality management systems and use is highly dependent on interpretation.

10. TCSEC

The US Department of Defense published its Trusted Computer System Evaluation Criteria (TCSEC) standard in December 1985, which allows qualifying information systems on the basis of security aspects. TCSEC classifies IT systems into groups on the basis of security aspects, qualifying the effectiveness of security control built in the information processing systems on the basis of protection levels of different strengths. The classification requires qualification to be performed in four areas: security policy, accountability, assurance and documentation.

11. ITSEC

The first version of ITSEC (Information Technology Security Evaluation Criteria) was elaborated jointly by England, France, the Netherlands and Germany in 1990, as a European counterpart of TCSEC. In respect of its principles and requirements, ITSEC basically agrees with TCSEC. However, in addition to the security classes interpreted in the same way as TCSEC, ITSEC also determines security classes for the relevant types of IT systems for which it determines the basic security features of TCSEC.

12. Various ISO standards

(i) ISO 9000

These are a set of high-level, customer-oriented, auditable standards (ISO 9000, 9001 and 9004) for quality management systems intended to ensure control, repeatability and good documentation of processes (not products). Well established and mature they enjoy global prestige and can be applied enterprise wide. Though they can cover software development, IT operations and services considerable adaptation when used in IT organizations is required. Focus is on repeatability and consistency of processes, not directly on the quality of those processes.

However they do not address the issues of analyzing a process and finding root causes of problems

(ii) ISO/IEC 15504 (SPICE)

In June 1991, the ISO/IEC JTC1/SC7 initiated a study on the need for a software process assessment standard. The results of this study drove the establishment of the Software Process Improvement and Capability determination (SPICE) project in 1993 to standardize and improve on the existing software assessment methodologies. The SPICE project is to address all processes involved in software acquisition, development, operation, supply, maintenance, and support and has been created to be aligned closely with "Software Life Cycle Processes."

(iii) ISO/IEC 17799:2000

The international standard was published by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Essential parts of the international standards labelled as *Information Technology—Code of Practice For Information Security Management* were developed and published by the British Standards Institution, labelled as BS 7799-1:1999. ISO/IEC 17799: 2000 provides information to parties responsible for implementing information security within an organization. It can be seen as a basis for developing security standards and management practices within an organization to improve reliability on information security in inter organizational relationships.

(iv) ISO/IEC TR 13335

ISO/IEC TR 13335 *Information Technology—Guidelines for the Management of IT Security* is a technical report published by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). The report provides guidance on aspects of IT security management providing an introduction to security concepts and models. It contains information on identifying and analysing communication-related factors that should be taken into account when introducing network security

13. NIST (National Institute of Standards and Technology)

The Computer Security Resource Center (CSRC) of the National Institute of Standards and Technology (NIST), a department of the US Department of Commerce has published *Generally Accepted Principles and Practices for Securing Information Technology Systems*, a

collection of principles and practices to establish and maintain system security.

14. TickIT

TickIT is a certification scheme developed to apply ISO9001 to deal with the special requirements of software development The TickIT initiative came about as a result of a report commissioned by the British Department of Trade and Industry (DTI) to review the state of software quality and development in industry. TickIT is mainly aimed at the UK market

15. Malcolm Baldrige National Quality Program

It is a broad high-level framework for quality in seven areas: company leadership, strategic planning, customer and market focus, information and analysis, human resources, process management and business results. It rates each of these, in terms of approach, execution and results, on a scale from 0 to 100. However it doesn't address process details; doesn't say how to achieve quality and doesn't directly address IT processes and issues.

16. Six Sigma

Developed by Motorola Inc it is a statistical process-improvement method focusing on quality from a customer's or user's point of view and defines service levels and measures variances from those levels. Projects go through five phases: define, measure, analyze, improve and control. The Design for Six Sigma variant applies this method's principles to the creation of defect-free products or services, rather than the improvement of existing ones. It has a data-driven approach towards finding the root causes of business problems and solving them and takes into account the cost of quality best applied for relatively homogeneous, repeatable activities such as call center or help desk operations. Design for Six Sigma can help develop good software specifications. Originally designed for manufacturing environments; may be difficult to apply to processes that aren't already well defined and measurable. Can improve a process but doesn't the right process to begin with.

17. AICPA Statement on Auditing Standards 55 and 78

The AICPA's Statement on Auditing Standards (SAS) 55/78 pertains to the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted auditing standards. The SAS 55/78 definition of internal control is identical to that of the COSO report. In addition to the three COSO objectives of internal control (efficiency and effectiveness of operations, accuracy of financial reporting, compliance

with applicable laws and regulations), SAS 55/78 also emphasizes the testing of relevant financial reporting and operational controls in order to assess whether the assets of an entity are adequately safeguarded.

As with the other internal control frameworks, SAS 55/78 states that, "Internal control, no matter how well designed and operated, can only provide reasonable assurance to management and the board of directors regarding the achievement of an entity's control objectives."

What are the keys to a successful Control Assessment Program?

The basic keys for making a Control assessment program a successful venture in any organisation is to take care of the following:

- The most important part of any Control assessment program is the need to obtain the encouragement and support of senior management. This is more applicable to internal audit than to external audit. Without their backing, lower levels of management will not be anywhere near as likely to take the process seriously. Without serious participation, a Control assessment program could be viewed as a waste of time.
- The second key to a successful Control assessment program is to ensure senior management support through effective demonstrations of the potential for significant gains in operational efficiency and effectiveness, and reductions in exposure to financial, regulatory, and other significant risks. These demonstrations can be supported by success stories at various organisations that have implemented successful Control assessment programs. Articles written about Control assessment may need to be referred to, and senior management may have to be better educated on the objectives of internal controls.
- The third key to a successful Control assessment program is proper training of auditors in the skills necessary to facilitate assessment. Till now, auditors have interacted with organisation staff and management on a one-on-one basis or in small group meetings. Auditors were not typically required to facilitate discussion by other groups. However, as Control assessment becomes more and more the norm in leading-edge companies, the demand for IT auditors as well as non-IT auditors who possess Control assessment facilitation skills will be significantly enhanced.

Auditors must also be highly knowledgeable about the particular internal control framework(s) adopted by an organisation's audit department. Therefore, training of both IT and non-IT auditors on the details of the applicable internal control framework(s) is also critical.

A fourth key to Control assessment success is having the proper tools. These tools include a private conference room or training room with flipcharts, marking pens, whiteboards or chalkboards, and other typical training materials, in addition to automated tools such as a laptop computer, etc.

Conclusion

Though all these frameworks/standards cover various aspects regarding controls in IT environment it is CoBIT which addresses the full spectrum of IT governance. Moreover since the audit guidelines in CoBIT are auditor oriented it is a more suited framework for Information Systems auditors. However as some of the other standards are highly specific and describe the controls in a more detailed manner than CoBIT, as in BS7799 (Information Security) and CMM (Acquisition & Human Resource Planning), these may have to be considered to complement CoBIT.

Glossary

Access path - Sequence of hardware and software components significant to access control. Any component capable of enforcing access restrictions or any component that could be used to bypass an access restriction should be considered part of the access path. The access path can also be defined as the path through which user requests travel, including the telecommunications software, transaction processing software, application program, etc.

Access privileges - Precise statements that define the extent to which an individual can access computer systems and use or modify the programs and data on the system, and under what circumstances this access will be allowed.

Application - A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support. Depending on the work for which it was designed, an application can manipulate text, numbers, graphics, or a combination of these elements.

Application programmer - A person who develops and maintains application programs, as opposed to system programmers who develop and maintain the operating system and system utilities.

Audit risk - The risk that information or financial reports will contain material errors that the auditor may not detect.

Audit trail – A serious of records either in hard copy or in electronic format that provide a chronological record of user activity and other events that show the details of user and system activity. Audit trails can be used to document when users log in, how long they are engaged in various activities, what they were doing and whether any actual or attempted security violations occurred.

Authentication - The act of verifying the identity of a user and the user's eligibility to access computerised information. Designed to protect against fraudulent activity.

Authorized program facility - An operating system facility that controls which programs are allowed to use restricted system functions.

Backdoor - An undocumented way to gain access to a program, data, or an entire computer system, often known only to the programmer who created it. Backdoors can be handy when the standard way of getting information is unavailable, but they usually constitute a security risk.

Batch processing - A mode of operation in which transactions are accumulated over a period of time, such as a day, week, or month, and then processed in a single\e run. In batch processing, users do not interact with the system while their programs and data are processing as they do during interactive processing.

Biometric authentication - The process of verifying or recognising the identity of a person based on physiological or behavioural characteristics. Biometric devices include fingerprints, retina patterns, hand geometry, speech patterns and keystroke dynamics.

Bridge - A device that allows two networks, even ones dissimilar in topology, wiring, or communications protocols, to exchange data.

Client/server model - A design model used on a network where individual workstations (clients) and shared servers work together to process applications. In this model, certain functions are allocated to the client workstations and the server. Typically, the server provides centralised, multi-user services, whereas the client workstations support user interaction.

Cold site - An IS backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternative computing location.

Communications program - A program that enables a computer to connect with another computer and exchange information by transmitting or receiving data over telecommunications networks.

Communications protocol - The standards that govern the transfer of information among computers on a network.

Compatibility - The capability of a computer, device, or program to function with or substitute for another make and model of computer, device, or program. Also, the capability of one computer to run the software written to run on another computer. Standard interfaces, languages, protocols, and data formats are keys to achieving compatibility.

Compensating control - An internal control that reduces the risk of an existing or potential control weakness that could result in errors or omissions.

Computer architecture - A general term referring to the structure of all or part of a computer system. The term also covers the design of system software, such as the operating system, as well as refers to the combination of hardware and basic software that links the machines on a computer network. Computer architecture refers to an entire structure and to the details needed to make it functional. Thus, computer architecture covers computer systems, circuits, and system programs, but typically does not cover applications, which are required to perform a task but not to make the system run.

Computer facility - A site or location with computer hardware where information processing is performed or where data from such sites are stored.

Computer-related controls - Computer-related controls help ensure the reliability, confidentiality and availability of automated information. They include both general controls, which apply to all or a large segment of an

entity's information systems and application controls, which apply to individual applications.

Confidentiality - Ensuring that transmitted or stored data are not read by unauthorised persons.

Configuration management - The control and documentation of changes made to a system's hardware, software and documentation throughout the development and operational life of the system.

Contingency plan - Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failure, or disaster.

Control environment - The control environment is an important component of an entity's internal control structure. It sets the "tone at the top" and can influence the effectiveness of specific control techniques. Factors that influence the control environment include management's philosophy and operating style, the entity's organizational structure, methods of assigning authority and responsibility, management's control methods for monitoring and following up on performance, the effectiveness of the Inspector General and internal audit, personnel policies and practices, and influences external to the entity.

Control Objectives for Information and Related Technology (CoBIT) - A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.

Control risk - Risk that a material misstatement that could occur in an assertion will not be prevented, or detected and corrected on a timely basis by the entity's internal control structure.

Cryptography - The science of coding messages so they cannot be read by any person other than the intended recipient. Ordinary text—or plain text—and other data are transformed into coded form by encryption and translated back to plain text or data by decryption.

Data administration - The function that plans for and administers the data used throughout the entity. This function is concerned with identifying, cataloguing, controlling, and coordinating the information needs of the entity.

Database - A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, or making decisions. Any collection of information that serves these purposes qualifies as a database, even if the information is not stored on a computer.

Database administrator (DBA) - The individual responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users to the database. Additional

responsibilities include operation, performance, integrity, and security of the database.

Data definition - Identification of all fields in the database, how they are formatted, how they are combined into different types of records, and how the record types are interrelated.

Data dictionary - A repository of information about data, such as its meaning, relationships to other data, origin, usage, and format. The dictionary assists management, database administrators, systems analysts, and application programmers in effectively planning, controlling, and evaluating the collection, storage and use of data.

Data Mining - Using of computer programs to search repeatedly through huge amounts of data, usually stored in a database, looking for useful patterns for use in guiding decision making and forecasting the effect of those decisions.

Data processing - The computerised preparation of documents and the flow of data contained in these documents through the major steps of recording, classifying, and summarising.

Data validation - Checking transaction data for any errors or omissions that can be detected by examining the data.

Data warehouse - A generic term for a system used to store, retrieve, and manage large amounts of data. A database, often remote, containing recent snapshots of corporate data that can be used for analysis without slowing down day-to-day operations of the production database.

Decision support system (DSS) - An information system or analytic model designed to help managers and professionals to be more effective in their decision-making.

Detection risk - The risk that the auditor will not detect a material misstatement that exists in an assertion.

Digital signature – A piece of information, a digitised form of a signature that provides sender authenticity, message integrity and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Distributed processing - A mode of operation in which processing is spread among different computers that are linked through a communications network.

Dumb terminal - A terminal that serves only as an input/output mechanism linking a user with the central computer. This type of terminal does not have an internal processor.

Download - Process of transferring data from a central computer to a personal computer or workstation.

Electronic data interchange (EDI) - A standard for the electronic exchange of business documents, such as invoices and purchase orders. Electronic data

interchange eliminates intermediate steps in processes that rely on the transmission of paper-based instructions and documents by performing them electronically, computer to computer.

Encryption - The transformation of data into a form readable only by using the appropriate key, held only by authorized parties.

End user computing - Any development, programming, or other activity where end users create or maintain their own systems or applications.

Environmental controls - This subset of physical access controls prevents or mitigates damage to facilities and interruptions in service. Smoke detectors, fire alarms and extinguishers and uninterruptible power supplies are some examples of environmental controls.

Financial information system - An information system that is used for one of the following functions: (1) collecting, processing, maintaining, transmitting and reporting data about financial events, (2) supporting financial planning or budgeting activity, (3) accumulating and reporting cost information, or (4) supporting the preparation of financial statements.

Firewall - Firewalls are hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorised users to access and transmit privileged information and deny access to unauthorised users.

Flowchart - A diagram of the movement of transactions, computer functions, media, and/or operations within a system. The processing flow is represented by arrows between symbolic shapes for operation, device, data file, etc. to depict the system or program.

Gateway - In networks, a computer that connects two dissimilar local area networks, or connects a local area network to a wide area network, minicomputer, or mainframe. A gateway may perform network protocol conversion and bandwidth conversion.

General controls - General controls are the structure, policies and procedures that apply to an entity's overall computer operations. They include an entity wide security program, access controls, application development and change controls, segregation of duties, system software controls and service continuity controls.

Hacker - A person who attempts to enter a system without authorisation from a remote location.

Hot site - A fully operational off-site data processing facility equipped with both hardware and system software to be used in the event of a disaster.

Inherent risk - The susceptibility of an assertion to a material misstatement, assuming that there are no related internal controls.

Integrity - With respect to data, its accuracy, quality, validity and safety from unauthorised use. This involves ensuring that transmitted or stored data are not altered by unauthorised persons in a way that is not detectable by authorised users.

Interface - A connection between two devices, applications, or networks or a boundary across which two systems communicate. Interface may also refer to the portion of a program that interacts with the user.

Internal control - A process, effected by agency management and other personnel, designed to provide reasonable assurance that (1) operations, including the use of agency resources, are effective and efficient; (2) financial reporting, including reports on budget execution, financial statements, and other reports for internal and external use, are reliable; and (3) applicable laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorised acquisition, use, or disposition. Internal control consists of five interrelated components that form an integrated process that can react to changing circumstances and conditions within the agency. These components include the control environment, risk assessment, control activities, information and communication and monitoring.

ISO 17799 – Originally released as part of the British Standard for Information Security in 1999 as the Code of Practice for Information Security Management, which in October 2000 was elevated by the International Organisation for Standardisation to an international code of practice for information security management. This standard defines information confidentiality, integrity and availability controls in a comprehensive information security management system.

Legacy system - A computer system, consisting of older applications and hardware that was developed to solve a specific business problem. Many legacy systems do not conform to current standards, but are still in use because they solve the problem well and replacing them would be too expensive.

Library - In computer terms, a library is a collection of similar files, such as data sets contained on tape and/or disks, stored together in a common area. Typical uses are to store a group of source programs or a group of load modules. In a library, each program is called a member. Libraries are also called partitioned data sets (PDS). Library can also be used to refer to the physical site where magnetic media, such as a magnetic tape, is stored. These sites are usually referred to as tape libraries.

Library control/management - The function responsible for controlling program and data files that are either kept on-line or are on tapes and disks that are loaded onto the computer as needed.

Local area network (LAN) - A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables a device to interact with any other on the network. Local area

networks (LAN) commonly include microcomputers and shared (often expensive) resources such as laser printers and large hard disks. Most modern LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.

Logic bomb - In programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.

Logical access control - The use of computer hardware and software to prevent or detect unauthorised access. For example, users may be required to input user identification numbers (ID), passwords, or other identifiers that are linked to predetermined access privileges.

Mainframe computer - A multi-user computer designed to meet the computing needs of a large organisation. The term came to be used generally to refer to the large central computers developed in the late 1950s and 1960s to meet the accounting and information management needs of large organizations.

Management controls - The organisation, policies and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organisation's mission, (3) programs and resources are protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported and used for decision-making.

Master file - In a computer, the most currently accurate and authoritative permanent or semi-permanent computerised record of information maintained over an extended period.

Material weakness - A material weakness is a reportable condition in which the design or operation of the internal controls does not reduce to a relatively low level the risk that losses, non-compliance, or misstatements in amounts that would be material in relation to the principal statements or to a performance measure or aggregation of related performance measures may occur and not be detected within a timely period by employees in the normal course of their assigned duties.

Materiality - An auditing concept regarding the relative importance of an amount or item. An item is considered as not material when it is not significant enough to influence decisions or have an effect on the financial statements.

Modem - Short term for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system. It also determines the speed at which information can be transmitted and received.

Naming conventions - Standards for naming computer resources, such as data files, program libraries, individual programs and applications.

Network - A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables, or temporary connections made through telephone or other communications links. A network can be as small as a local area network consisting of a few computers, printers and other devices, or it can consist of many small and large computers distributed over a vast geographic area.

Network administration - The function responsible for maintaining secure and reliable network operations. This function serves as a liaison with user departments to resolve network needs and problems.

Network architecture - The underlying structure of a computer network, including hardware, functional layers, interfaces and protocols (rules) used to establish communications and ensure the reliable transfer of information. Because a computer network is a mixture of hardware and software, network architectures are designed to provide both philosophical and physical standards for enabling computers and other devices to handle the complexities of establishing communications links and transferring information without conflict. Various network architectures exist, among them the internationally accepted seven-layer open systems interconnection model and International Business Machine (IBM) Systems Network Architecture. Both the open systems interconnection model and the Systems Network Architecture organise network functions in layers, each layer dedicated to a particular aspect of communication or transmission and each requiring protocols that define how functions are carried out. The ultimate objective of these and other network architectures is the creation of communications standards that will enable computers of many kinds to exchange information freely.

Node - In a local area network, a connection point that can create, receive, or repeat a message. Nodes include repeaters, file servers and shared peripherals. In common usage, however, the term node is synonymous with workstation.

Nonrepudiation – Assurance that a party cannot later deny originating data. It is the provision of proof of the integrity and origin of the data and can be verified by a third party. A digital signature can provide nonrepudiation.

Object code - The machine code generated by a source code language processor such as an assembler or compiler. A file of object code may be immediately executable or it may require linking with other object code files, e.g., libraries, to produce a complete executable program.

Off-the-shelf software - Software that is marketed as a commercial product, unlike custom programs that are privately developed for a specific client.

On-line - A processing term that categorizes operations that are activated and ready for use. If a resource is on-line, it is capable of communicating with or being controlled by a computer. For example, a printer is on-line when it can be used for printing. An application is classified as on-line when users interact

with the system as their information is being processed as opposed to batch processing.

On-line transaction monitor - In the mainframe environment, software that provides online access to the mainframe.

On-line transaction processing - On-line transaction processing records transactions as they occur.

Operating system - The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware and presents a default interface to the user when no application program is running.

Operational controls - These controls relate to managing the entity's business and include policies and procedures to carry out organisational objectives, such as planning, productivity, programmatic, quality, economy, efficiency and effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) meets its goals, (2) maintains quality standards and (3) does what management directs it to do.

Owner - Manager or director with responsibility for a computer resource, such as a data file or application program.

Partitioned data set (PDS) - Independent groups of sequentially organised records, called members, in direct access storage. Each member has a name stored in a directory that is part of the data set and contains the location of the member's starting point. PDSs are generally used to store programs. As a result, many are often referred to as libraries.

Password - A confidential character string used to authenticate an identity or prevent unauthorised access.

Physical access control - This type of control involves restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment.

Piggy-backing - A method of gaining unauthorised access to a restricted area by entering after an authorised person but before the door closes and the lock resets. Piggy-backing can also refer to the process of electronically attaching to an authorised telecommunications link to intercept transmissions.

Platform - The foundation technology of a computer system. Typically, a specific combination of hardware and operating system.

Port - An interface between the CPU of the computer and a peripheral device that governs and synchronises the flow of data between the CPU and the external device.

Privileges - Set of access rights permitted by the access control system.

Processing - The execution of program instructions by the computer's central processing unit.

Production control and scheduling - The function responsible for monitoring the information into, through and as it leaves the computer operations area and for determining the succession of programs to be run on the computer. Often, an automated scheduling package is utilised in this task.

Production data - The data that supports the organisation's operational information processing activities. It is maintained in the production environment as opposed to the test environment.

Production environment - The system environment where the organisation performs its operational information processing activities.

Production programs - Programs that are being used and executed to support authorised organisational operations. Such programs are distinguished from "test" programs which are being developed or modified, but have not yet been authorised for use by management.

Profile - A set of rules that describes the nature and extent of access to available resources for a user or a group of users with similar duties, such as accounts payable clerks.

Protocol - In data communications and networking, a standard that specifies the format of data as well as the rules to be followed when performing specific functions, such as establishing a connection and exchanging data.

Prototyping - A system development technique in which a working model of a new computer system or program is created for testing and refinement.

Quality assurance - The function that reviews software project activities and tests software products throughout the software life-cycle to determine if (1) the software project is adhering to its established plans, standards and procedures and (2) the software meets the functional specifications defined by the user.

Real-time system - A computer and/or a software system that reacts to events before they become obsolete. This type of system is generally interactive and updates files as transactions are processed.

Regression testing - Selective retesting to detect faults introduced during modification of a system.

Reliability - The capability of hardware or software to perform as the user expects and to do so consistently, without failures or erratic behaviour.

Remote access - The process of communicating with a computer located in another place over a communications link.

Remote job entry (RJE) - With respect to computer systems with locations geographically separate from the main computer centre, submitting batch processing jobs via a data communications link.

Reportable condition - Reportable conditions include matters coming to the auditor's attention that, in the auditor's judgment, should be communicated

because they represent significant deficiencies in the design or operation of internal controls, which could adversely affect the entity's ability to meet its internal control objectives.

Risk assessment - The identification and analysis of possible risks in meeting the organisation's objectives that forms a basis for managing the risks identified and implementing deterrents.

Risk management - A management approach designed to reduce risks inherent to system
development and operations.

Router - An intermediary device on a communications network that expedites message delivery. As part of a LAN, a router receives transmitted messages and forwards them to their destination over the most efficient available route.

Security administrator - Person who is responsible for managing the security program for computer facilities, computer systems, and/or data that are stored on computer systems or transmitted via computer networks.

Security management function - The function responsible for the development and administration of an entity's information security program. This includes assessing risks, implementing appropriate security policies and related controls, establishing a security awareness and education program for employees and monitoring and evaluating policy and control effectiveness.

Security plan - A written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer resources.

Security program - The security program is an entity wide program for security planning and management that forms the foundation of an entity's security control structure and reflects senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures and monitoring the effectiveness of these procedures.

Sensitive information - Any information that, if lost, misused, or accessed or modified in an improper manner, could adversely affect the national interest, the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Server - A computer running administrative software that controls access to all or part of the network and its resources, such as disk drives or printers. A computer acting as a server makes resources available to computers acting as workstations on the network.

Simultaneous peripheral operations on-line (SPOOL) - In the mainframe environment, a component of system software that controls the transfer of data between computer storage areas with different speed capabilities. Usually, an intermediate device, such as a buffer, exists between the transfer source and the destination (e.g., a printer).

Smart card - A credit card sized token that contains a microprocessor and memory circuits for authenticating a user of computer, banking, or transportation services.

Sniffer - Synonymous with packet sniffer - A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

Social engineering - A method used by hackers to obtain passwords for unauthorised access. Typically, this involves calling an authorised user of a computer system and posing as a network administrator.

Software life cycle - The phases in the life of a software product, beginning with its conception and ending with its retirement. These stages generally include requirements analysis, design, construction, testing (validation), installation, operation, maintenance and retirement.

Source code - Human-readable program statements written in a high-level or assembly language, as opposed to object code, which is derived from source code and designed to be machine-readable.

Spooling - A process of storing data to be printed in memory or in a file until the printer is ready to process it.

Stand-alone system - A system that does not require support from other devices or systems. Links with other computers, if any, are incidental to the system's main purpose.

Steering committee – A management committee assembled to sponsor and manage various projects such as an information security program.

Substantive testing - Substantive testing is performed to obtain evidence that provides reasonable assurance of whether the principal statements and related assertions, are free of material misstatement. There are two general types of substantive tests: (1) substantive analytical procedures and (2) tests of details.

System administrator - The person responsible for administering use of a multi-user computer system, communications system, or both.

System analyst - A person who designs systems.

System development life cycle (SDLC) methodology - The policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.

System programmer - A person who develops and maintains system software.

System software - The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. It includes the operating system and utility programs and is distinguished from application software.

System testing - Testing to determine that the results generated by the enterprise's information systems and their components are accurate and the systems perform to specification.

Tape library - The physical site where magnetic media is stored.

Tape management system - Software that controls and tracks tape files.

Test facility - A processing environment isolated from the production environment that is dedicated to testing and validating systems and/or their components.

Time-sharing - A technique that allows more than one individual to use a computer at the same time.

Token - In authentication systems, some type of physical device (such as a card with a magnetic strip or a smart card) that must be in the individual's possession in order to gain access. The token itself is not sufficient; the user must also be able to supply something memorised, such as a personal identification number (PIN).

Transaction - A discrete activity captured by a computer system, such as an entry of a customer order or an update of an inventory item. In financial systems, a transaction generally represents a business event that can be measured in money and entered in accounting records.

Transaction file - A group of one or more computerised records containing current business activity and processed with an associated master file. Transaction files are sometimes accumulated during the day and processed in batch production overnight or during off-peak processing periods.

Trojan horse - A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.

Unit testing - Testing individual program modules to determine if they perform to specification.

UNIX - A multitasking operating system originally designed for scientific purposes which have subsequently become a standard for midrange computer systems with the traditional terminal/host architecture. UNIX is also a major server operating system in the client/server environment.

User identification (ID) - A unique identifier assigned to each authorized computer user.

User profile - A set of rules that describes the nature and extent of access to each resource that is available to each user.

Utility program - Generally considered to be system software designed to perform a particular function (e.g., an editor or debugger) or system maintenance (e.g., file backup and recovery).

Validation - The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

Virus - A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files.

Wide area network (WAN) - A group of computers and other devices dispersed over wide geographical areas that are connected by communications links.

Workstation - A microcomputer or terminal connected to a network. Workstation can also refer to a powerful, stand-alone computer with considerable calculating or graphics capability.

Worm - An independent computer program that reproduces by copying itself from one system to another across a network.

Bibliography

- Information Systems Audit and Control Association Standards and Guidelines
- INTOSAI IT Audit Courseware, 2001
- National Audit Office, Financial Audit Manual – Module T9 – Audit in an IT environment
- CoBIT.
- IFAC Auditing standards,
- Ron Weber, Information Systems Controls and Audit, Prentice Hall,
- Martin A Krist, Standard for Auditing Computer Applications, Auerbach Publications.
- Federal Information Systems Controls Audit Manual, GAO, 1999
- BS 7799: IT – Code of Practice for Information Security Management,
- Capability Maturity Model (SW) framework of Carnegie Mellon University
- James R Hickman, Practical IT Auditing, Warren, Gorham and Lamont,
- Donald Warren, Lynn Edelson and Xenia Parker, Handbook of IT Auditing, Warren, Gorham and Lamont,
- Doug Dayton, IT Audit Handbook, Prentice Hall,
- Jack Chaplan, Auditing Information Systems, Wiley Publications,
- Donn Barker, Fighting Computer Crime, Wiley Publications,
- System Audit, Dr. M Revathy Sriram
- Treasury Board of Canada Publications

Contributors to the IT Audit Manual :

Subhashini Srinivasan

Vani Sriram CISA, CIA

Rajesh K Goel CISA, CIA

G Srinivas CISA, CIA

Dr Ashutosh Sharma CISA

IT Audit Manual peer reviewed by

Anupam Kulshreshtha CISA, CISM, CIA

N Nagarajan CISA, CISM, CIA

Subir Mallick

A K Ojha CISA

IT Audit Manual preparation support Group

Namashivayam CISA

K P Singh

Murali Krishnan

B J Chanda

S C Naithani