IT Audit Manual

Table of Contents

1. Introduction

The incessant development of information technology has changed the way organizations work in many ways. 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have made way for the online data entry of computerized applications; the locks and keys of filing cabinets have been replaced by passwords and identification codes that restrict access to electronic files. The implementation of innovative technology has helped organizations to improve the efficiency of their bussines processes and considerably increase their data processing and transmission capacity, but has also introduced new vulnerabilities that need to be controlled. Each new vulnerability needs to be controlled; assessing the adequacy of each control requires new methods of auditing. With the increase in the investment and dependence on computerised systems by the auditees, it has become imperative for audit to change the methodology and approach to audit because of the risks to data integrity, abuse, privacy issues etc. An independent audit is required to provide assurance that adequate measures have been designed and are operated to minimize the exposure to various risks.

2. Definition and Objectives

IT audit is the examination and evaluation of an organization's information technology infrastructure, policies and operations. IT audit can be considered the process of collecting and evaluating evidence to determine whether a computer system safeguards assets, maintains data integrity, allows organizational goals to be achieved effectively and uses resources efficiently.

The objectives of IT audit include assessment and evaluation of processes that ensure:

i. Asset safeguarding –'assets' which include the following five types of assets:

1. Data objects in their widest sense, (i.e., external and internal, structured and non- structured, graphics, sound, system documentation etc).
2. Application system is understood to be the sum of manual and programmed procedures.
3. Technology covers hardware, operating systems, database management systems, networking, multimedia, etc.
4. Resources to house and support information systems, supplies etc.
5. Staff skills, awareness and productivity to plan, organize, acquire, deliver, support and monitor information systems and services.

ii. Ensures that the following seven attributes of data or information are maintained:

1. 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.
2. Efficiency - concerns the provision of information through the optimal (most productive and economical) usage of resources.
3. Confidentiality - concerns protection of sensitive information from unauthorized disclosure.
4. 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.
5. Availability - relates to information being available when required by the business process, and hence also concerns the safeguarding of resources.
6. 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 organization.

7. Reliability of information

3. Phases of the Audit Process

The audit process includes the following steps or phases:

1. Planning.
2. Definition of audit objectives and scope.
3. Evidence collection and evaluation.
4. Documentation and reporting.

3.1 Planning

3.1.1 Preliminary assessment and information gathering.

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.

3.1.2 Understanding the organization.

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

- Organizational function and the operating environment.

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

.

- Organizational Structure.
  The IT auditor needs to obtain an understanding of the organizational hierarchy as well as the structure and hierarchy of the IT department.
- Criticality of IT systems.
  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 organization. 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.

- Nature of hardware and software used.
  Understanding the hardware details of the organization 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. The auditor needs to understand the type of software used in the organization. The auditor needs to collect details of operating systems, application systems and Database Management Systems used in the organization. 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. Preliminary assessment of hardware and software would enable planning the audit approach and the resources required for evidence collection.

- Nature and extent of Risks affecting the systems.

The auditor can gather the required information by:

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

The extent of the knowledge of the organization and its processes required by the auditor will be determined by the nature of the organization and the level of detail at which the audit work is being performed.Knowledge of the organization should include the business, financial and inherent risks facing the organization. It should also include the extent to which the organization 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.

3.2 Risk assessment to define audit objective and scope.

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. The three security goals of any organization are Confidentiality, **I**ntegrity and **A**vailability. Risk assessment is a systematic consideration of:

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

It is therefore necessary in audit to understand that there is a pay off between the costs and the risks, which are acceptable to the management. For instance, the management might consciously decide that offsite storage is not required in view of low risks, which are acceptable to the business. In other words it is important to study the management perspective and laid down policy before audit comes to a conclusion of acceptable and unacceptable risks. Therefore, any assessment of the soundness of the IT system will necessarily have to study the policies and process of risk management adopted by an organization.

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

1- Inventory the information systems in use in the organization and categorise them.
2- Determine which of the systems impact critical functions or assets.
3- Assess what risks affect these systems and the severity of impact on the business.
4- Based on the above assessment decide the audit priority, resources, schedule and frequency.

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. Policies, procedures, practices and organizational structures put in place to reduce risks are referred to as internal controls. 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. Elements of controls that should be considered when evaluating control strength are classified as Preventive, Detective and Corrective with the following characteristics.

Preventive	• 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.

The auditor should ordinarily make a preliminary evaluation of the controls and develop the audit plan on the basis of this evaluation. 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. Although 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.

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 performance of a system or a specific programme.
- Review of the security of the IT systems.
- Examine the system development process and the procedures followed at various stages involved therein.

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

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

Scope defines the boundaries of the audit. Determining the scope of the audit is a part of audit planning and 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.

3.3 Evidence collection and evaluation

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

under audit. Data collection techniques should be carefully chosen. The auditors should have a sound understanding of techniques and procedures chosen.

3.3.1 Types of Audit Evidence.

When planning the IT audit work, the auditor should take into account the type of the audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability. 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)

Physical evidence is obtained by observing. 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.
Physical access controls are designed to protect the organization from unauthorised access. The following methods are generally employed for collection of audit evidence.

1-Interviews

Auditors can use interviews to obtain both qualitative and quantitative information during evidence collection work. System analysts and programmers can be interviewed to obtain a better understanding of the functions and controls embedded within the system. 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.

2-Questionnaires

Questionnaires have been used traditionally to evaluate controls within systems. Auditors can also use questionnaires to flag areas of system weakness during evidence collection. Similarly, questionnaires can be used to identify areas within an information system where potential inefficiencies exist. Some general guidelines of questionnaires need to be kept in view. Questions must be specific. Must be used a language which is commensurate with the understanding of the intended person. Leading questions, presumptuous questions and leading questions must be avoided.

3- Flowcharts

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

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

4-Analytical Procedures

Analytical procedures use comparisons and relationships to determine whether account balances appear reasonable. 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..

3.3.2 Tools of evidence collection.

With increased necessity for certification of systems, there is also an increase in the availability of tools which the IT auditors can use.

Generalised Audit Software.

Generalised audit software provide 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- organization, selection and extraction of data, various data analysis function and reporting functions. They are used to examine the existence, accuracy, completeness, consistency and timeliness of data the quality of processes embedded within an application system analytical review to monitor key audit indicators such as trend analysis. 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.

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.

Utility Software.

This software performs frequently used functions such as copy, sort, disc search, disc format etc.

Specialised Audit Software.

This is software written to fulfil a specific set of audit tasks. Most well developed systems have embedded audit modules, which essentially comprise routines that throw up alerts as well as information to ensure continued dependence on controls.

Concurrent Audting Tools.

Concurrent Auditing techniques are used 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.

3.4 Documentation and Reporting.

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 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 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.

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

3.4.1 Structure of the report.

The report should be timely, complete, accurate, objective, convincing, and as clear and concise as the subject permits. The report can be broadly structured under the following headings:

Introduction

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.

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. In reporting the audit's objectives, auditors should explain the aspects of performance examined. 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,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. 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 and describe the criteria used.

Audit Results.

Findings

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.

Conclusions

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. 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.

Recommendations

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. 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

Noteworthy Accomplishments

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.

Limitations

It is important to mention in the audit report, limitations that were faced by audit.

4. The Audit Methodology

4.1 IT Controls

The capabilities of computer systems have advanced rapidly over the past several decades. In many organizations, 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.

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.

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 organizations 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. 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 organization from fraudulent activity and encompasses substantiating the reported results of processing transactions or activities.

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.

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 organization. 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 organization's site, buildings, computer rooms and each piece of IT hardware. Logical access controls are restrictions imposed by the computer software.

***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.

***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. 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.

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.

Nature of hardware and software used

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. 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.

***Weak Security*:** Information systems security should be a concern of both users and management. However, security, for many companies, is not a top priority.

***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 addition, confidential data that is transmitted over public lines should be encrypted.

***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.

***Inadequate training*:** Organizations 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 organizations make to train both end users and IT professionals.

IT controls can be classified in two broad categories:

1-General Controls.

2- Application Controls.

General controls include controls over data centre operations, system software acquisition and maintenance, access security, and application system development and maintenance. 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 organization's IT infrastructure, including any IT related policies, procedures and working practices.

General IT controls include:

- Organization 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 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 to ensure all transactions have been posted completely and accurately.

Application Controls include:

- Controls over the input of transactions.
- Controls over processing.
- Controls over output.
- Controls over standing data and master files.

Audit of General Controls.

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. Following are the major categories of general controls that an auditor should consider. The IT auditor may use the information for evaluating the practices adopted by auditee organization. In order to facilitate the auditor's evaluation, sample audit checklists in a tabular format have been summarised in the appendix of this manual.

.

4.2 Audit of General Controls

4.2.1 IT Operations Control.

4.2.1.1 Control Objectives

The roles of IT operations include the following:

- ***Capacity Planning***: 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.
- ***Back-ups***: backups of data and software should be carried out by IT operations staff on a regular basis.
- ***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.

4.2.1.2 Risks

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)
- Loss or corruption of financial applications or the underlying data files: may result from improper or unauthorised use of system utilities.
- 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.
- Users' problems remaining unresolved due to a poor help-desk function.

4.2.1.3 Audit Procedures

4.2.1.3.1 Service Level Agreements.

It is increasingly common for IT departments to draw up and enter into service level agreements (SLA) with the rest of the organization, 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. The structure and level of service specified in a SLA will depend upon the working practices and requirements of each organization. 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.
- Service hours.
- Service availability (percentage availability, maximum number of service failures and the maximum downtime per failure);
- User support levels.
- Performance (response times, turnaround times);
- Security.
- Restrictions.

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

4.2.1.3.2 Manegement control and supervision.

Operations staff should be supervised by the management. The organization'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. 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. As with most logging systems, a large quantity of data can be produced in a short period. Recommending that an organization 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 organization should develop procedures (e.g. a program) to report exceptions or anomalies.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.

.

4.2.1.3.3 Operations Documentation

The organization 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;
- System restart and recovery procedures.

The organization 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. 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. The auditor should bear in mind the level and detail of documentation will vary from one organization to another, and will depend on factors such as the size of the organization, 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 organization running office automation software would probably have less detailed and extensive documentation.

4.2.1.3.4 Problem Management

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.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.

4.2.1.3.5 Network Management and Control

A range of controls is required where an organization 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.
- Establishment and monitoring of security controls specific to computer network.

4.2.2 Physical Control (Access and Environment)

4.2.2.1 Control Objectives

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.The entity's IT security policy should include consideration of physical and environmental risks.

4.2.2.2 Risks

Physical

- Accidental or intentional damage by staff.
- Theft of computers or their individual components.
- Power spikes or surges which may cause component damage and the loss or corruption of data.

- Copying or viewing of sensitive or confidential information.

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

4.2.2.3 Audit Procedure

To ensure that adequate internal controls exist to protect the business's assets and resources, the organization 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.

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 controls reduce the risk of unauthorised persons gaining access to the computer equipment. The auditor should identify controls which would restrict access to the organization's site, the computer rooms, terminals, printers and data storage media. Common physical access controls include the use of locked doors, CCTV, intruder alarms, combination keypads and security guards. Access to the organization'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. Newer devices such as biometric devices use voice recognition, facial features, hand geometry, fingerprints, retina scan etc to control physical access to the system. 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. 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.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. Automatic moisture detectors may be used to alert IT staff of potential water ingress.Uninterruptible

power supplies reduce the risk of system disruption and damage and can allow continued processing following a power cut. Some 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.

4.2.3 Logical Access Control

4.2.3.1 Control Objectives

The objective of logical access controls is to protect the 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

4.2.3.2 Risks

- 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.
- Employees are not barred/ restrained from performing incompatible functions or functions beyond their responsibility.

4.2.3.3 Audit Procedure

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. 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 organization makes use of wide area networks and global facilities such as the Internet. Logical access controls usually depend on the in-built security facilities available under the operating system or hardware in use.Additional access controls can be gained through the appropriate use of proprietary security programs. 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. Organizations 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. 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. 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.

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 that require protection:

- Data Files - These may consist of transaction files or databases.
- Applications – Unrestricted access increases the risk that the applications will be subject to unauthorised amendment leading to fraud, data loss, and corruption.
- Password Files- 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. Even where the identifier and password of an ordinary user are obtained, the concept whereby users are held accountable for their actions is bypassed.
- System software and utilities – 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.
- Logs - Log files are used to record the actions of users and hence provide the system administrators and organization management with a form of accountability. If log files are inadequately protected, a hacker, fraudster etc. could delete or edit it to hide his/her actions.

4.2.4 Program Change Controls

4.2.4.1 Control Objectives.

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. 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. 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.

Reasons for system changes.

After systems are implemented the system maintenance phase begins. Systems rarely remain the same for long. Changes may be requested for the following reasons:

- To enhance functionality: everyday system users may not be content with the functionality of the system like 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 for 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
- To improve security: IT security personnel: identified weaknesses in system security may result in requests for change which should improve security.
- Routine updates.
- Changes in requirements: changes in legislation, business requirements or business direction may require the financial system to be amended.

4.2.4.2 Risks

Change controls are put in place to ensure that all changes to systems configurations are authorised, tested, documented, controlled, the systems operate as intended.

- The risks associated with inadequate change controls are as follows:
- Unauthorised changes
- Implementation problems
- Erroneous processing and reporting
- User dissatisfaction
- Maintenance difficulties
- Use of unauthorised hardware and software

4.2.4.3 Audit Procedure

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

- Procedures for management authorization
- Thorough testing before amended software is used in the live environment
- Management review of the effects of any changes
- Maintenance of adequate records
- The preparation of fallback plans
- The establishment of procedures for making emergency changes

There should be procedures for recording all requests for change (RFC). 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 priority of changes is determined by assessing the cost of the change and impact on the business and its resources.

4.3 Audit of Application Controls.

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, and complete and recorded. 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.

- Application controls may be divided into:
- Input controls
- Processing controls
- Output controls
- Master/Standing Data File controls.

4.3.1 Input Controls.

4.3.1.1 Control Objectives

The objective of Input control is to ensure that the procedures and controls reasonably guarantee that:

- The data received for processing are genuine, complete, not previously processed, accurate and properly authorized.
- 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.

4.3.1.2 Risks

- 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

4.3.1.3 Audit Proceure

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.

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.The organization 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 organization also gains better control of resources. 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. 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:

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.

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 organization 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 organization also gains better control of resources. 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. 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 control matrices
- Obtaining printout of user permissions
- Reviewing audit logs of changes in permissions

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. IT applications may have in-built controls which automatically check that data input is accurate and valid. 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. 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. 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.

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

- **Rejected by the system** -Where transactions are rejected outright, the organization 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.
- **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.

4.3.2 Processing Controls

Processing controls ensure complete and accurate processing of input and generated data.

4.3.2.1 Control Objectives

4.3.2.2 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
- The computer processes are auditable.

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.

4.3.2.3 Risks

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

- Unauthorised changes or amendments to the existing data
- Absence of audit trail rendering, sometimes, the application unauditable

4.3.2.4 Audit Procedure.

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. The auditor should ensure that there are controls to detect the incomplete or inaccurate processing of input data. 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. Computerised systems should maintain a log of the transactions processed. The transaction log should contain sufficient information to identify the source of each transaction. Errors detected during processing should be brought to the attention of users. On-line systems should incorporate controls to monitor and report on unprocessed or unclear transactions. There should be procedures which allow identifying and reviewing all unclear transactions beyond a certain age

4.3.3 Output Controls

Output controls are incorporated to ensure that computer output is complete, accurate and correctly distributed.

4.3.3.1 Audit Objectives

Output controls ensure that all output is:

- Produced and distributed on time
- Physically controlled at all times, depending on the confidentiality of the document
- Errors and exceptions are properly investigated and acted upon

4.3.3.2 Risks

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 organization.
- Non-availability of the data at the time when it is desired.
- Even sometimes, the information which may be of very confidential nature may go to the wrong hands.

4.3.3.3 Audit Procedure

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. 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. Output files should be protected to reduce the risk of unauthorised amendment. A combination of physical and logical controls may be used to protect the integrity of computer output. Output from one IT system may form the input to another system. 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.

4.4 Network and Internet Controls

4.4.1 Control Objectives

The majority of systems encountered in medium to large scale organizations use either local or wide area networks to connect users. The use of networks is increasing and bringing organizations 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
- Allow users to access the systems from remote locations.

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. 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.

4.4.2 Risks

Where the organization's systems are connected to networks, there is potentially a greater risk of unauthorised access by unathorised users which may lead 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
- Fraud
- 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 organization, e.g. The organization may rely on the local telephone company for isdn lines
- 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
- Contravention of copyright

4.4.3 Audit Procedure

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 organization must place great emphasis on logical access and administrative controls. The logical access controls will vary from one organization to another depending upon the identified risks, the operating system, the network control software in use and the organization's network and communications policies. Before carrying out a review of the organization's logical access and network controls, the auditor should review any technical material or publications on the organization's systems. For example, if the IT auditor happens to have a copy of a publication on security and controls for the organization's network operating system, he should review it before visiting the organization's premises.

Controls which the auditor may encounter include:

- Network security policy: this may be a part of the overall IT security policy
- Network documentation: the organization should have copies of documentation describing the logical and physical layout of the network
- These are usually treated as confidential
- Logical access controls: these are especially important and the organization should ensure that logons, passwords and resource access permissions are in place

- 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
- Access by external consultants and suppliers should be monitored. It may be the case that the organization 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
- Data encryption: In certain circumstances the organization 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
- 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

4.5 Internet Controls

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.
- Have as few user accounts as possible on the internet machine and change their passwords regularly.

4.5.1 Firewalls

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 can be set up to allow only specific Internet services and may provide additional services such as logging, authentication, encryption and packet filtering. 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

4.5.2 Internet Password Policy.

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. A good password policy can make a significant contribution to the security of computers attached to the Internet. Practicies like regular password change, use of complex passwords etc can be part of the internet password policy. 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. 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.

5. Appendix

5.1 Audit Checklist: List of Documents for understanding the system

The commencement of any audit is with the review of the background of the organization to understand its activities and the impact of IT on these activities. Along with the nature of organization, the audit party would be specifically interested in the background of IT systems in use in the organization. The following illustrative list of documents can be collected for understanding the system.

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

No.	List of documents
20	Test data and test results
21	Security set up for the system
22	Previous audit reports
23	Internal audit reports
24	User feed back about the system
25	Peer review reports

5.2 Audit Checklist:Criticality Assesment Tool

Multiple IT systems may be in use in an organization. The auditor may not be interested in auditing all the IT applications in an organization. The nature, extent, scope and rigour of the IT audit and the resources committed for the job are dependent upon the subjective assessment of the risk parameters or in other words, criticality of the application. The process of establishing the criticality of a system is subjective. The following criticality assessment tool may be used to categorise the applications based on criticality.

1	**Does the system relate to any of the following**			
	Business Critical Operations For example, Airline/Railway reservations, trading operations, telecom, banking operations, bill	(30)		
	Support Functions	(25)		
	For example, Payroll, Inventory, Financial Accounting, Procurement, Marketing etc.			
2	**Investment made in the System**			
3	**General state of computerization in the entity. The entity has computerized**			
	Most of the Business processes	(30)		
	Most of the Accounting and Financial Processes	(25)		
	No business process	(0)		
4	**Number of PCs/Desktops used for the system**			
	More than 100	(30)		
	More than 50, less than 100	(25)		
	More than 20, less than 50	(15)		
	More than 10 less than 20	(10)		
	Less than 10	(5)		
5	**Is the system on the network?**			

	Yes		
	No		
	If the system is on the network, is it connected to		
	Internal LAN and/or on intranet?	(20)	
	WAN and MAN and/or on extranet?	(25)	
	Web based /public domain?	(30)	
6	**The system is functioning at**		
	Only one location	(10)	
	More than one, less than 5 locations	(20)	
	Name of the Office:		
	Preliminary Information		
	More than 5 locations	(30)	
	Is proposed to be expanded in more than one location	(25)	
7	**The entity is dependant on the system in as much as**		
	Outputs are used for business critical operations /revenue generation	(30)	
	Outputs are manually checked ***before*** making payments/raising bills	(10)	
	Outputs are used to prepare Financial Statements	(15)	
	Outputs are not used at all for payment/revenue	(0)	
8	**Even though the system does not deal with financial functions, it processes data of public interest. The nature of data is such that, wrong data may lead to :**		
	Failure of business	(30)	
	Erosion of credibility of the Organization	(15)	
	Financial loss to the entity	(25)	
	None of the above	(0)	
9	**Do the public have access to such data either through web or any other means?**		
	Yes, Public can view the data in a dynamic manner	(15)	
	No, Public cannot view the data	(0)	
	Public can transact on-line	(30)	
10	**Does the System make use of direct links to third parties e.g. EDI**		
	Yes	(20)	
	No	(0)	
11	**Does the Organization have dedicated IT Staff**		
	Nil	(0)	

	Less than 10	(10)	
	More than 10, less than 30	(20)	
	More than 30, less than 70	(25)	
	More than 70	(30)	
12	**Approximately how many persons can be termed as the end-users of the system?**		
	Name of the Office:		
	Preliminary Information		
	Less than 5	(0)	
	More than 5, less than 25	(10)	
	More than 25, less than 70	(20)	
	More than 70, less than 150	(25)	
	More than 150	(30)	
13	**The system is in operation for**		
	More than 10 years	(5)	
	Less than 10 years but more than 5 years	(10)	
	Less than 5 years but more than 2 years	(20)	
	Less than 2 years	(20)	
14	**The system is based on**		
	Batch Processing	(10)	
	On Line Transaction Processing	(25)	
15	**Are there formal change management procedures?**		
	Yes	(0)	
	No	(20)	
	How often changes are made to the applications		
	More than 5 times in a year	(30)	
	Less than 5 times in a year more than twice in a year	(20)	
	Less than twice in a year	(10)	
	Not even once in a year	(5)	
16	**Does the entity have a documented and approved security policy?**		
	Yes	(5)	
	No	(20)	
17	**Does the entity use any security software?**		
	Yes	(5)	
	No	(20)	

18	**Does the entity have a Systems Security Officer?**		
	Yes	(5)	
	No	(10)	
	Name of the Office:		
	Preliminary Information		
19	**Does the entity have a documented and**		
	Disaster Recovery Plan?		
	Yes	(0)	
	No	(20)	
20	**Volume of data in the system(including off line data) is**		
	More than 10 GB	(25)	
	More than 2 GB less than 10 GB	(15)	
	Less than 2 GB	(10)	
	Less than 1 GB	(5)	
	Total Score		

5.3 Audit Checklist: Collection of specific information on IT Systems

The Audit management may require to collect some specific information on the IT systems. The following questionnaires may be used to collect the information at the time of conduct of audit.

5.3.1 Form 1

1. Name of the auditee organization:	
2. Date on which information collected :	
3. Name of the IT Application and broad functional areas covered by the IT Application:	
4. Department Head of the Audit Organization: Name: Phone No:	

Email:	
5. Department Head of the Auditee Organization: Name: Phone No: Email:	

6. Information Systems in-charge: Name: Phone No: Email:	
7. What is (are) the location(s) of the IT system installation(s)?	
8. State the category of IT system architecture:	A. Mainframe based Minicomputer based PC based Others (please specify)
	B. File server system Client server system Distributed processing system Webbased/EDI Others (specify)

9. State the category of IT application. (Please indicate the choice(s) applicable):	Accounting system Financial management system Inventory/Stock Management Decision support system/MIS Manufacturing/ Engineering Payroll Personnel and Administration Marketing Sales e-Governance
10. Whether the above IT application has got a bearing on the financial and accounting aspects of the organization?	Yes No

11. Software used (the Version may also be specified):	
Operating system(s)	
Network software	
Communication Software	
DBMS / RDBMS	
Front end tool	
Programming Language(s)	
Bespoke (Vendor developed)	
Utility Software	
Any other	

12. Is the IT system a mission critical system or an essential system?	Mission critical system[β] Essential system[γ]					
13. Has the application system been developed in house or by outsourcing?	In house					
14. In case of outsourcing, specify the name of agency and the contracted amount:						
15. When was the system made operational?	**MM**		**YYYY**			

16. Number of persons engaged for operation of the system?	01 – 10 11 – 25 26 – 50
17. What is the average volume of transactional data generated on a monthly basis in terms of storage space	
19. Does the system documentation provide for an audit trail of all transaction processed and maintained?	Yes No
20. Are the manuals as indicated available?	
a. Users documentation manual	Yes No
b. Systems and programming documentation manual	Yes No
21. Is there any system in place to make modifications to the application being used on a regular basis to support the function?	Yes No
22. Does the organization transmit/receive data to/from other organizations:	Receive Transmit No

5.3.2 Form 2

22. Details of all Hardware items including the number of terminals etc. employed: _____ _____ _____ _____
23. Details of networking hardware employed:

_____ _____ _____ _____
24. Are more than one IT Application(s) running on the same Hardware? If Yes, specify the name(s) of such IT Application(s) _____ _____ _____ _____

5.3.3 Form 3

26. What is the current status of development of IT system if it is still under development? (Tick the appropriate box indicating the current stage of development of IT Application)	Feasibility study stage User requirement Specification stage Design stage Development stage Testing stage Parallel run (if any) Implementation stage
27. What is the projected cost for the IT system?	_____
28. What is the target date for completion?	_____(MM/YY)

5.4 Audit Check List: Check list for risk assesment

The following checklist gives an illustrative list of questions to be asked regarding various aspects of IT systems in order to form an opinion about the risk levels. These checklists

may have to be modified by the auditor based on an understanding of the organization and the application to be audited.

No	Item	Respo	
		Y	N
	Management & Organization		
1	Is there a strategic IT plan for the organization based on Business needs?		
2	Is there a steering committee with well defined roles and Responsibilities?		
3	Does the IT department have clear cut and well defined goals And targets?		
4	Is there a system of reporting to top management and review In vogue?		
5	Is there a separation of duties and well defined job Characteristics in the IT Department?		
7	Are there appropriate policies and procedures in relation to Retention of electronic records?		
8	Where the organization uses third parties to process data, does It have appropriate procedures in place to address associated risks?		
9	Are there procedures to update strategic IT plan?		
	Personnel policy		
10	Whether criteria are used for recruiting and selecting Personnel?		
11	Whether a training needs analysis is done at periodical Intervals?		
12	Whether training programmes are periodically held to update Knowledge?		
13	Whether organization's security clearance process is adequate?		
14	Whether employees are evaluated based on a standard set of Competency profiles for the position and evaluations are held on a periodic basis?		
15	Whether responsibilities and duties are clearly identified?		
16	Whether backup staff is available in case of absenteeism?		
17	Whether there is a rotation of staff policy in key areas where uninterrupted functioning is essential		
	Security		

18	Is there a strategic security plan in place providing centralized Direction and control over information system security?		
19	Is there a centralised security organization responsible for Ensuring only appropriate access to system resources?		
20	Is there a data classification schema in place?		
21	Is there a user security profile system in place to determine Access on a "need to know basis"?		
22	Is there an employee indoctrination/training system in place That includes security awareness, ownership responsibility and virus protection requirements?		
23	Whether cryptographic modules and key maintenance Procedures exist, are administered centrally and are used for all external access and transmission activity?		
24	Whether preventative and detective control measures have Been established by management with respect to computer viruses?		
25	Whether change control over security software is formal and Consistent with normal standards of system development and maintenance?		
26	Whether password policy exists		
27	Whether access to the VoiceMail service and the PBX system Are controlled with the same physical and logical controls as for computer systems?		
28	Whether access to security data such as security management, Sensitive transaction data, passwords and cryptographic keys is limited to a need to know basis?		
	Physical & Logical access		
29	Whether facility access is limited to least number of people?		
30	Whether "Key" and "including ongoing card reader" Management procedures and practices are adequate, update and review on a least-access-needed basis?		
31	Whether access and authorisation policies on entering/leaving, Escort, registration, temporary required passes, surveillance cameras as appropriate to all and especially sensitive areas are adequate?		
32	Is there a periodic and ongoing review of access profiles, Including managerial review?		
33	Whether security and access control measures include Portable and/or off-site used information devices?		
34	Whether review occurs of visitor registration, pass assignment, escort, person responsible for visitor log book to ensure both check in and out occurs and receptionist's understanding of security procedures?		

35	Is there a system of reviewing fire, weather, electrical warning And alarm procedures and expected response scenarios for various levels of environmental emergencies?		
36	Is there a system of reviewing air conditioning, ventilation, Humidity control and expected response scenarios for various loss or unanticipated extremes?		
37	Whether health, safety and environmental regulations are Being complied with?		
38	Whether physical security is addressed in the continuity plan?		
39	Whether specific existence of alternative infrastructure items necessary to implement security: • uninterruptible power source (UPS) • alternative or rerouting of telecommunications lines • alternative water, gas, air conditioning, humidity resources		
40	Are there procedures to update physical and logical access Procedures?		
	Business Continuity & Disaster Recovery		
41	Have the business critical systems been identified?		
42	Has an appropriate business continuity plan been developed, Documented and approved?		
43	Whether regular review and update of the plan has been Carried out?		
44	Are back up copies of data files and programs taken Regularly?		
45	Are the documents of the system and disaster recovery plan Appropriately backed up?		
46	Are back up copies held in secure locations both locally and Remote from the computer site?		
47	Are the back-up and recovery procedures appropriately Tested?		
48	Are the business systems and operations effectively designed To minimize disruption?		
49	Are there procedures to update business continuity and Disaster recovery plan?		
	Hardware		
50	Is there an organization policy for upgrading the hardware based on technology changes?		
51	Is there an effective preventive maintenance program in place for all significant equipment?		

52	Is equipment downtime kept within reasonable limits (say <5%)		
53	Is a reasonable effort made to acquire data centre and networking hardware that is compatible with the existing environment?		
54	Is anyone in the IT organization responsible for identifying potentially unnecessary equipment and taking appropriate action?		
55	Is a formal inventory of all IT hardware available?		
56	Are there procedures to update documentation whenever Changes made in the hardware?		
	Software		
57	Is the software used covered by adequate licences?		
58	Is the source code available and if so, accessible at what level?		
59	Is there a system of recording changes to the applications?		
60	Are these changes properly authorized?		
61	Whether emergency change procedures are addressed in Operation manuals?		
62	Whether proper testing was carried out and results recorded before final implementation of application?		
63	Is there an exception reporting system in place?		
64	In the case of bought out software are there agreements in place for maintenance and service?		
65	Is there a system of obtaining user feed back and reporting action taken thereon to management?		
66	Is the application design documented?		
67	Whether the programs are documented?		
68	Is the testing methodology documented?		
69	Whether operations procedures are documented?		
70	Whether user manuals are available?		
71	Do manuals include procedures for handling exceptions?		
72	Are there procedures to update documentation when an Application changes?		
	Data Management		

73	Whether for data preparation the following exist: • data preparation procedures ensure completeness, accuracy and validity • authorisation procedures for all source documents • separation of duties between origination, approval and conversion of source documents into data • periodic review of source documents for proper completion and approvals occurs • source document retention is sufficiently long to allow reconstruction in the event of loss, availability for review and audit, litigation inquiries or regulatory requirements		
74	Whether for data input whether the following exist: • appropriate source document routing for approval prior to entry • proper separation of duties among submission, approval, authorisation and data entry functions • audit trail to identify source of input • routine verification or edit checks of input data as close to the point of origination as possible • appropriate handling of erroneously input data • clearly assign responsibility for enforcing proper authorisation over data		
75	For data processing: Whether programmes contain error prevention, detection, correction routines		
76	Whether error handling procedures include: • correction and resubmission of errors must be approved • individual responsibility for suspense files is defined • suspense files generate reports for non-resolved errors • suspense file prioritization scheme is available based on age and type		

77	Whether logs of programmes executed and transactions Processed/rejected for audit trail exist?		
78	Whether there is a control group for monitoring entry activity And investigating non-standard events, along with balancing of record counts and control totals for all data processed?		

79	Whether written procedures exist for correcting and Resubmitting data in error including a non-disruptive solution to reprocessing?		
80	Whether resubmitted transactions are processed exactly as Originally processed?		