CHAPTER VIII

AUDIT APPROACH

Overview

Approach to audit in a computerised environment, as already mentioned, is different from the approach in a manual system. While specific controls and audit concerns are associated with each computerised environment, there is a general approach recommended for a computerised environment. In this chapter, that aspect is discussed.

The examination upon which the report of attestation is based is known as Audit. The individual doing such work is usually referred to as auditor. An auditor may be an internal auditor or an external auditor. The internal auditor is appointed by the Management and he reports to them. External auditor or a statutory auditor in companies is appointed by the shareholders, at the annual general meeting and under the Company Law. The auditor gives his report under the statute to the shareholders.

"The Statement of responsibilities of the Internal Auditors" was issued by the Institute of Internal Auditors originally in 1947. Subsequently in 1978, "Standards for the professional practice of internal auditing" was issued.

The main points covered were:

* Independence
* Professional proficiency
* Scope of work
* Performance of audit work
* Management of the Internal Audit Departments.

The more important aspects under this head are as follows:

**Independence**

Internal auditors should be independent of the activities they audit.

**Objectivity**

Internal auditors should be objective in performing audits.

The internal auditing department’s Knowledge, skills and disciplines - The internal auditing department should possess or should obtain the knowledge, skills and disciplines needed to carry out its audit responsibilities.

**Supervision**

The internal auditing department should provide assurance that internal audits are properly supervised.
The Internal auditor

Continuing Education

Internal auditors should maintain their technical competence through continuing education.

Due professional care

Internal auditors should exercise due professional care in performing internal audits.

Reliability and integrity of information

Internal auditors should review the reliability and integrity of financial and operating information and the means used to identify measure classify and report such information.

Compliance with policies, plans, procedures, laws and regulations: Internal auditors should review the systems established to ensure compliance with those policies, plans, procedures, laws and regulations which could have a significant impact on operations and reports and should determine whether the organisation is in compliance.

Safeguarding of assets

Internal auditors should review the means of safeguarding assets and as appropriate verify the existence of such assets.
Examining and evaluating information

Internal auditors should collect, analyse, interpret and document information to support audit results.

Quality assurance

The director of internal auditing should establish and maintain a quality assurance program to evaluate the operations of the internal auditing department.

The internal audit department provides assistance to Management by analysing and reporting on the activities reviewed by them. Internal auditors can be concerned with any phase of the business activity of the organisation. Information systems is an important activity of the organisation which also forms the basis for accounting and financial statement. So to attain the objective of rendering assistance to management in the effective discharge of the responsibilities, auditors activities will include the following:

- Reviewing and evaluating the soundness, adequacy of controls associated with accounting, finance and other activities satisfying himself regarding the extent of compliance with established policies and procedures.
- Evaluating reliability of management data and information developed, reviewing information systems, record and process financial data.

The auditing standards pronounced by the professional bodies are discussed in greater detail in the Chapter on Auditing Standards. SAS No.47 addresses audit risk. Audit risk is defined at the financial statement level as "the risk that the auditor
may unknowingly fail to appropriately modify his opinion on financial statements that are materially mis-stated."

The risk that material error exists is divided into:

(i) Inherent risk and
(ii) Control risk

The components of audit risk could be described as follows:

**OVERALL AUDIT RISK**

The inherent risk could be identified with a knowledge of the business and an understanding of its transactions.

**Internal control risk**

The internal control risk is assessed when the internal auditor by establishing the effectiveness of the control system. The basic objective of any internal accounting control system is to provide assurance that all transactions are complete and accurate.
In a computerised environment, the auditor needs to review and evaluate the associated internal control systems to determine whether adequate controls exist to assure the auditor that all transactions are processed correctly and completely.

It is in this background when an auditor is performing his duty in a computerised environment, unless he is aware of acceptable standards for controls associated with a particular computerised environment, he would not be able to evaluate its adequacy. Consequently his assuring himself that all transactions are processed correctly and completely does not arise.

In large organisations auditors are permitted to rely on the internal auditors opinion under certain circumstances. In addition they have their own responsibility as they are certifying the correctness of financial statements which themselves are prepared on the computer. It will thus be observed that an auditor, whether he be internal or external, he should be knowledgeable about specific controls. Specific controls would be different depending upon the specific computerised environment.

The objectives of the audit in a computerised environment are only the same. However, in a computerised environment in view of the internal controls being different, the audit mechanism for evaluating such controls has to be different too.

**PROBLEM AREAS**

All organisations - small and big - have computerised their accounting system. Larger organisations are having sophisticated management information systems. The technological developments have been growing very fast. Auditing skills have remained stagnant. The internal auditors do not have in their team any staff member
who possess the necessary skills and knowledge to audit in a computerised environment. The position regarding external auditors who are big firms of long standing and who have amongst their clients large organisations with very high turnover are also not having necessary skills and knowledge to perform an effective audit.

The present practices adopted by the auditors is limited to extensive checking of hard copies of computer statements. While extensive checking of the contents of the computer statements is undertaken, no attempts are being made to satisfy themselves about the basic correctness and completeness of the Statements. In a computerised environment auditing is generally divided into three categories:

i. Auditing around the computer

ii. Auditing through the computer

iii. Auditing with the computer

i. Auditing around the computer could be resorted to when the computer could be dealt with like a Black Box and the print outs are exhaustive and comprehensive so that every input transactions can be traced to an output document.

ii. Auditing through the computer is a situation when computer cannot be treated as a Black Box. Transactions are sometimes visible and sometimes invisible. The audit trail itself becomes a bit more complex. In such situations, the program logic should be tested.

iii. In auditing with the computer, auditors' skills and knowledge are so high that he takes advantage of the capabilities of a computer and uses his own program or a software to evaluate the correctness and the completeness of
computer statements. In the present day computer technology has developed to such an extent that it would be most appropriate for an auditor to perform an audit with the computer. However, the methodology adopted by all the auditors without exception is to adopt the approach of auditing around the computer while the situation demands an auditing with the computer. The auditors are not performing any of the functions.

i. Understanding the computer system i.e. to know the type of hardware and software used and the operating system used.

ii. A list of applications

iii. Studying the system flow-charts.

Verifying whether there is adequate documentation for programs, whether there are any formal procedures documented for changes and programs, understanding the built-in controls as also the compensating controls for each of the applications, testing the programs and other procedures to evaluate the existence and adequacy of controls, disaster recovery plan, reporting to the management regarding their opinion on the audit performed.

In the absence of awareness of the management regarding the necessity to have an audit of the computerised environment, they do not have the internal audit to perform audit of the computerised environment.

In the absence of official statements from the professional bodies, external auditors are not performing the audit of the computerised environment.
There are reported and unreported cases of frauds occurring in a computerised environment.

Due to lack of knowledge, competence and skills and also as so far neither the Management nor the auditor has been sued by a third party for dereliction of duty for not evaluating the controls in a computerised environment the present outdated practices and methods of auditing are continuing in a sophisticated environment of using the latest information technology.

Lack of awareness of the risks and vulnerabilities associated with computerisation generally and specifically with certain environments was apparent in very many examples. Infalliability of the computer is confused with the notion that all computer output will be error free and complete and correct and so no questions need be asked.

There have been instances when the accountants within the company with the cooperation of the computer staff have been able to produce computer print outs to suit the audit requirements and auditors of the particular concern certified the accounts based on such statements in the firm belief that they have checked "computer outputs".

In another organisation while there was supposedly a control on the total entries to be passed under each category there was no creation of a suspense file for entries which were rejected. Letters were written to the concerned departments with a copy to internal audit regarding the entries rejected. It was a shocking revelation to note that the matter ended there. In the same organisation the
vulnerability was exploited by collusion between a staff member of the computer department incharge of control totals and a clerk is one of the outstation depots. A cash entry was passed, supposedly, to support a deposit in the ban of the depot. Bank reconciliations done six months later, did not help to reveal the intermediary frauds. Even the internal auditors as also the external auditors were totally unaware of the goings on. Neither of them had any knowledge of the approach to audit when the accounts are computerised.

In another organisation preparation of invoices were computerised with the built in control to reject such records which did not comply with the control supposedly built into the program regrdign type of product, sales tax classification, excise duty classification etc. Surprisingly the computer system staff had built the logic that once the record was rejected, the rejected records would be rectified by the user department and fed into the computer and hence it would be waste of computer efficiency to check again! This led to a situation when if a computer record had to bypass the supposedly built in controls they must have it rejected initially. In a discussion on controls, with Finance Controller this point was brought out when the Financial Controller was surprised of the loophole in the control. He hastened to have it corrected. Again, however, neight the internal auditors nor external auditors were aware of this situation.

In yet another organisation while preparing stock valuation reports on the computer, the wrong master file regarding the market value was loaded which was compared with correct master file of costs. The logic of comparing the cost or market value whichever is lower was no doubt correctly applied. But the stock valuation was wrong as wrong market file was loaded.
The objective of an audit is to evaluate the adequacy or otherwise of the internal controls and to report on the same. The objective of an audit does not change irrespective whether the environment is manual or computerised. The method of satisfying oneself with controls that need to exist do exist and they are adequate, however change when the environment changes from the manual.

In a computerised environment different situations may arise:

(a) While the data originates from the user department, the recording and processing of the same takes place in a separate department, normally called the data processing department.

(b) The user departments may be provided with terminals, either intelligent or dumb. All these terminals are net-worked and a file server or two is maintained in a separate department under the control of a separate manager.

(c) A Database Management System might have been introduced adding yet another complexity to a local area network.

Whatever may be the method that is adopted, there are certain changes which have taken place as distinct from the manual system:

i. Transactions are not always visible

ii. The input for certain computer runs or the output of certain other computer with the result intermediary results may not be always available in a hard copy.

iii. With each type of computerisation, there are certain controls associated with them to ensure accuracy, completeness, integrity and security of the system.
In view of the above the auditor necessarily will have to be knowledgeable about the relevant controls that are applicable to a specific computerised environment so that he is in a position to evaluate the adequacy or otherwise of the same. He would thus be able to give a comprehensive report about his opinion of the internal controls, in the information system which is being used by the organisation. The auditor, either internal or external, is expected to report either to the management or to the shareholders as the case may be, about he being satisfied or otherwise about the adequacy of the controls. In the case of adequacy, he should be in a position to quantify the consequences or the magnitude of such a weakness. To achieve the above mentioned objectives, the auditor should adopt the proper approach, as mentioned by William E. Perry.¹

**STEP 1**

The initial step that the auditor should take would be to scope the environment, primarily to understand the environment in which the computer applications run and also to assess the audit scope and decide on the areas in which the audit will be conducted. Scoping helps the auditor to collect adequate background information to perform an effective audit function. The various tasks that the auditor would be required to perform are:

(a) Understand the audit objective

(b) Define the scope of the assignment to obtain necessary background information.

The above tasks may be effectively performed by following the procedures given below:

The audit objective should be very clearly stated giving no room for any ambiguity. The scope of the assignment may be constrained as mentioned by William E. Perry, by four Ts—viz. Time, Talent, Tools and Travel. As is obvious, if the time is inadequate and the effort of travel is more than reasonable, the scope cannot necessarily be extensive. In addition, if the concerned staff do not have the necessary talent or though the staff may have the talent, if the necessary tools in the form of the software packages or utilities are not available or usable at the computer installation, the auditor would be constrained. This would be a contributory factor for deciding on the scope of the assignment.

The auditor should necessarily obtain the background information; this would enable him to put the objective of the audit in the proper perspective. The auditor should meet the concerned key personnel in the computer department as also the user’s department, he should acquire some knowledge if he does not already possess, so as to enable him to assess the possibility of any potential problems. The auditor should prepare suitable questionnaire which, when completed, would give him necessary information about the auditee being evaluated as also the computerised environment.

STEP 2
Understand the Information System

An information system would generally have the following ingredients: (a) Manual process; (b) Basic documents; (c) Computer processing; (d) Computer files
held in either in the hard disc/floppies, various inputs and outputs; the auditor must first obtain a overview of the information system by concentrating on the system objectives and identify flow of audit evidence. The procedures he could usefully follow to understand the information is stated below:

The information system would encompass both manual and automated processing. Hence, it is necessary to study the systems in the basic manual environment, the final computerised environment and the linkage between the two. A method which has been generally found effective to understand an information system is for the auditor to conduct a "systems walkthrough". This involves identification of all input transactions by the auditor and following these transactions through the various computer process. This information should generally be available in the documentation that the computer department is expected to maintain. The documentation would include a list of the various authorised applications with a systems flow-chart for the different applications like the payroll, inventory, financial accounting etc. Each of the systems documentation should have (a) program specifications (b) Listing of the source code, user manuals, operations procedure etc.

The auditor may obtain an application flow-chart from the organisation or develop one himself. A flow-chart is a pictorial representation of the computer process. The flow-chart helps in simplifying and presenting in a concise form large amounts of complex computer processing.

It is recommended that when the auditor prepares application flow-charts, they should be reviewed with the organisation's data processing department to ensure its accuracy and completeness.
STEP 3
Identify the audit risks

A risk can be defined as a potential loss or damage to an organisation. This is present in any environment and computerised environment is more vulnerable to risk if adequate steps are not taken to implement effectively. The functions that the auditor has to perform for identifying the audit risk would be by (a) identifying the possible risk inherent in the information systems (b) evaluate the magnitude of the risk and (c) prioritise the risk with reference to the importance from the auditor’s point of view.

Identifying the risks

It would be possible to identify the risks in a computerised environment only if the auditor and his team are familiar with the information system as also the computerised environment in which the particular information system operates. As mentioned earlier, a computerised environment has additional risks as compared to manual processing. It is necessary for the auditor to identify these risks. An illustrative but not necessarily an exhaustive list of all the risks generally associated with the computerised environment is as mentioned below:

Repetition of errors

While in a manual process errors are made individually, in a computerised environment if there is an error in a program, the error would be committed consistently for any number of transactions with greater speed.
Cascading of errors

An error in a particular part of a program may trigger an unrelated error in another part of the programme or applications systems may in its turn trigger yet another error; this type of error becomes more complicated when there is an integrated system.

Unreasonable processing

In the absence of human judgment, certain unreasonable processing is likely to take place. A junior individual on a very low salary may be given a computer job the value of which is ten times or hundred his entitlement. There may be an inventory application in which a quantity for a particular item may be denoted with a negative figure. Similarly due to wrong processing a cash account may also denote a negative balance.

Incorrect entry of data

Though properly prepared, may be wrongly entered into the computer. Even when data is generated and entered into the computer, at the same time, there is a possibility of errors creeping in.

Concentration of data

Unlike in a manual system when voluminous data is stored in different places, in a computerised environment the data is concentrated in a computer file. This gives room for the possibility of data being copied without even the owners of the data
being aware of the same. Sometimes this may result in the original data being
modified or deleted. When more and more data are stored in a centralised place, the
greater is the value for the data and greater is the vulnerability. The inability to
substantiate processing in the absence of proper audit it may be difficult to
substantiate the processing. It should be possible to trace the sources of transactions
and establish its integrity by means of control totals.

Concentration of responsibilities

Responsibilities which might have been separated for control purposes in a
non-computerised environment may get merged and get concentrated in a single
application. This necessitates the substitution of new controls to make up for the
previous separation of duties.

Determine the magnitude of risk

While quantitative ranking of the risk like whether it is high, medium or low
is adequate, it may be useful to quantify the same to facilitate effective presentation
to the management.

Prioritising the risks

It is important that the risks should be prioritised so that the auditor would
be able to prioritise his risks and suitably divide the resources among the various
risks.
STEP 4

Identifying audit evidence

Electronic evidence as distinct from the paper evidence has had a significant impact on the control process as also the audit process. As more and more evidence is becoming electronic to substantiate the evidence, it is necessary that not only the electronic evidence should be available, but it should be supported by adequate and relevant controls concerning its origination, recording and storage. The following table provides details regarding information systems audit evidence:

### INFORMATION SYSTEM AUDIT EVIDENCE

<table>
<thead>
<tr>
<th>Types of Evidence</th>
<th>Examples of Evidence in Automated System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization</td>
<td>* Supervisor key</td>
</tr>
<tr>
<td></td>
<td>* Automated authorization rules</td>
</tr>
<tr>
<td></td>
<td>* User signoff</td>
</tr>
<tr>
<td>Recording</td>
<td>* Data files/data bases</td>
</tr>
<tr>
<td></td>
<td>* System/program documentation</td>
</tr>
<tr>
<td></td>
<td>* Communication logs</td>
</tr>
<tr>
<td>Access to assets</td>
<td>* Passwords</td>
</tr>
<tr>
<td></td>
<td>* Security Systems</td>
</tr>
<tr>
<td></td>
<td>* Communication logs</td>
</tr>
<tr>
<td>Asset accountability</td>
<td>* Operator log</td>
</tr>
<tr>
<td></td>
<td>* DBMS log</td>
</tr>
<tr>
<td></td>
<td>* Program change control</td>
</tr>
<tr>
<td>Operational Performance</td>
<td>* Job accounting log</td>
</tr>
<tr>
<td></td>
<td>* Software/hardware monitors</td>
</tr>
<tr>
<td></td>
<td>* Failure/complaint reports</td>
</tr>
<tr>
<td>Satisfy goals and objectives</td>
<td>* Quality assurance reports</td>
</tr>
<tr>
<td></td>
<td>* Metrics</td>
</tr>
<tr>
<td></td>
<td>* Post-implementation review reports</td>
</tr>
</tbody>
</table>

It is very important to note that it is not only the computer technology but also the use to which the technology is put which decides the type of evidence that the auditor will need to look into. The auditor would be better advised in this connection to (i) make an exhaustive list of all the evidence produced by the computerised application system; most of the information should be available even at the stage when the auditor spends time to understand the information system and (ii) document the audit evidence. When documenting the evidence the major points that the auditor should note would be (1) Medium: It may be stored on a floppy or a hard disc or tape; (2) Location; the place where the computer media is stored. (3) Size and format: the size of the file as also the format of the records are important. (4) Period: the time for which the evidence would be stored before being discarded is very important. The auditor should ensure that the evidence is capable of being retained till such time he requires. The auditor should collect adequate information so that he would be able to develop his own software programme or use a computer utility so that he can analyse and list the electronic evidence for audit purposes.

**STEP 5**

**Identify key control points**

Key control points are points in a computer system where the risk is greatest and naturally control is most important. The generally accepted and easily usable strategies which can be adopted by the auditors are as follows:

i. Checklist

ii. Control flow charting

iii. Matrices
The questionnaires have many disadvantages as they tend to be very long and hence make it difficult to analyse. The Matrix is a good and effective strategy. This matrix provides list of controls to protect information systems against possible vulnerabilities. Control flow-charts are most effective. The tasks involved are: (1) Locate the risks on the control flow chart; (2) Document the key controls on the control charts; (3) Locating the controls on the control flow chart: The auditor who would have already identified the possible risks must match these risks with that part of the information systems in which the risk is the greatest. This matching would help in identifying the points where the risks need to be controlled or where the key control points are incorporated in a computerised system.

Document key control on the application flow chart

It would be necessary for the auditor to document the computer systems controls by concentrating on the key controls.

STEP 6
IDENTIFYING CONTROL WEAKNESSES

A weakness is a condition which in the auditor’s opinion could result in a loss; once it is identified, it can be tested to determine the magnitude of the potential control weaknesses.
Documenting for control weakness identification

Unlike manual systems which are inconsistent, computerised information systems are pre-determined and consistent. The three methods which could be used for documenting of control weaknesses are (a) control flow charting; (b) conflict matrix and (c) transactions-control matrices.

Preparation of a conflict matrix

This is an easy method for identifying when a single individual is vested with too much responsibility. The process involved in preparing the conflict matrix consists of identifying the people who have interest in information system and secondly identifying conflicting connections by means of the ability they have to manipulate. Processing the matrix is prepared by listing of the connections of one access of the people involved in the information systems in the other access.

Preparation of transactions control matrix

Transactions which involve economic events like cash, bank, receipts and payments should be considered for this matrix. The economic events are recorded on one access of the matrix while the information systems are recorded in the other access. Controls codifying each of these transactions are listed at the matrix intersection. This type of the matrix has the advantage of documenting the compensating controls.
Analysis and document potential control weaknesses

The control assessment consists of four ingredients.

First, identify the risk; control flow chart could help in identifying the risk.

Second, determine the magnitude of the risk;

Third, determine the strength of the controls; each of the controls should be assessed individually to enable the auditor to assess how strong it is.

Fourth, identify control weakness and document the same. The auditor should make cost-benefit analysis to ensure that cost of the control is not more than the magnitude of the loss due to the weakness.

Verifying the integrity of the computer files

The various steps in verifying the integrity of the computer files are:

i. Identifying the files for examination; this could be done by studying the systems flow chart. The files generally selected are those that would be needed to test control weaknesses.

ii. File documents.
File documents

Save the needed computer files. It is necessary for the auditor after having decided which file is needed to ensure that the file will be available at the time he plans to take or conduct the test.

iii. Verify the integrity of the file

This is done to ensure that the data on file is reconcilable to an independent control - the total or equivalent. Examples - control figures of subsidiary ledgers, overstatement of assets, understatements of liabilities. The file integrity may be performed independently or in conjunction with other audit tests. It is very important to note that the file integrity test should be personally performed by the auditors. Auditor's independence would be lost if the tests were developed and performed by the data processing people or by the user department. However, where the auditor does not have the necessary skills, he could rely on a third party.

iv. Verify the integrity of the data on the file

The auditor may use the software or utility and have the data on the file and have the same classified according to their requirements. Example: Accounts receivable file, classified as more than six months, less than six months; the balances which are beyond credit limits authorised etc; inventories as items which have not moved for more than a year or as A, B, C analysis.
STEP 8

CONDUCT AN AUDIT TEST

In countries where computerisation has been in existence for more than 50 years, as in the case of United States, Canada, Japan, Australia, etc. there are software in the category of generalised computer audit software. However, in our country we do not have the availability of such a software and also the necessary knowledge and skills to use such software is absent. However, the auditors are not handicapped by the absence of such a software. The controls used by the programmers and systems analysts to build in controls could be used by the auditors to conduct such tests.

STEP 9

CONCLUDING THE AUDIT

The objective of the audit is to evaluate the controls and give information on the adequacy or otherwise of the same. Hence, while concluding audit the auditor should determine the findings, develop recommendations and working out the details for the acceptance of those recommendations. The steps involved are:

(1) Develop audit findings; a finding is a comparison of existing situation with an ideal situation. A finding should contain the following information:

(i) factual situation observed by the auditor
criteria for judgment. The criteria in a computerised environment are the standards and guidelines and well-defined implementable controls specific to each environment;

(3) Effect of the condition

The auditor should compare the condition as it exists with the condition as it should exist and give an opinion on the effect it would have. (4) Develop audit recommendations: It is advisable that the auditor should discuss his recommendations with the auditee. It is well said that the best recommendation is the one that has been accepted prior to its being presented.

Writing the Audit Report

The audit report should be short, be bereft of terminology and jargon; it should contain a summary with explanatory material attached. The report should be positive and effective, giving suggestions about corrective actions to be taken in areas which have been prioritised.

ANALYSIS AND FINDINGS

A questionnaire based on standard literature of audit approach was prepared. Leading firms of Chartered Accountants were also selected with sample. All the firms and individual auditors have a wide variety of clients which include public limited companies, nationalised banks etc. Almost all their clients have computers in their
organisation. All the financial statements which are certified by these firms are prepared on the computer. A total sample of 30 auditors was selected.

The response to the questionnaire was personally collected. A summary of the response received on the questionnaire is enclosed.

An analysis discloses that none of the auditors are at present having confidence or the skills to perform an audit in a computerised environment. Further, they certified that the financial statements which are outputs from computers represent a true and fair view of the affairs of the company. A detailed discussion with them reveal that they are ignorant of specific controls in each types of the computerised environment; they rely on the management personnel of their clients’ organisation for the integrity of the information.

A further sample of 30 companies who are clients of one particular auditor’s firm was chosen. These firms are dealt with by different partners who have their own assistants who are qualified chartered accountants. A more detailed study based on the questionnaire was performed. It was revealing to note that neither the juniors of the firm nor the seniors have made any attempt to study the controls in the computerised environment of their clients. In all the cases the auditors were not even aware of the type of computer that was in their client’s organisation.

Information is an important asset of the organisation and the organisations are entirely dependent on the information produced by the computer. In all the organisations computerisation has been in existence for more than 15 years. The
auditors were not aware of the possible risks involved. They claim that the integrity of the people associated with computers in their client's organisation was unquestionable and hence they have no reason to feel concerned. It was also claimed that they had not come across any fraud situation. I conducted an independent study of a sample of 30 organisations and had personal discussions with the senior members of the staff, both in the computer division as also the finance departments. A statement is enclosed giving the risk factor involved. The computer-risk assessment procedure and the questionnaire have been adopted, as suggested in the book "Audit computer Security - A manual with case studies" by S. Rao Vallabhaneni, the data was gathered by providing the questionnaire to them earlier and meeting them later. The questionnaire was jointly compiled by me and the senior member of the computer department who did it with the approval and knowledge of the Finance Controller.

The risk value and the criterion weight are not based on any scientific evidence; they are based on intuition and graded according to the intensity of the risk. The risk ranking working sheet was prepared (Annexure H).

SUGGESTIONS FOR ORGANISATIONS

Knowledge of appropriate controls associated with specific computerised environments should be acquired by the auditors, whether they be internal or external. Managements who have the primary responsibility for controls should issue policies and guidelines in consultation with competent people, from within and from
outside consultants. The policies and guidelines should clearly lay down the procedures regarding

- Organisational and administrative controls
- Documentation standards
- Maintenance of security and integrity of files and data
- Procedures for disaster recovery planning
- Nominating a group for constantly monitoring the implementation of policies and procedures and ensuring that they are updated in keeping with the changed circumstances.

SUGGESTIONS FOR AUDITORS

It is long overdue for the auditors to become computer-literate. It is essential for them to have a thorough knowledge of control and security aspects associated with each computerised environment. This need for knowledge is immediate and long overdue. It would be desirable to have a EDP cell in all large audit firms. The staff of the EDP Cell needs to be trained and kept up to date on current technology in computers.

Where it is not possible to have a separate cell it would be advisable to rope in a consultant who has the necessary knowledge and experience. However, the auditor's basic responsibility regarding the need for satisfying himself about the adequacy of controls cannot be relegated or delegated due to non-availability of competent staff. With knowledge adequate to meet the situation, it is recommended
outside assistance can be sought. In special circumstances, when evaluation of assets needs to be done and certified, it is not uncommon to get a third party who is competent to do so to give a certificate based upon which the auditors themselves authenticate the financial statement. The same procedure needs to be adopted immediately.

If auditors and organisations do not wake up to the situation, frauds of serious consequence would take place. The chapter describing the "scenario" in other parts of the world has a short description of the crimes and frauds that have been reported in countries such as USA, UK and Australia.

Various charts depicting the average annual computer abuse, loss and computer crime loss, relative seriousness of frauds have been enclosed. These charts and reports should be eye-openers for managements of organisations and auditors to implement post-haste audit of and in computerised environment.