CHAPTER I

INTRODUCTION

Computers were originally used by organisations that could afford them. The initial costs and the subsequent running costs were affordable only by a few. The reason of affordability of the computer only by a few is something of the past.

The present scenario is totally different. Every organisation is owning a computer of some type or the other. The other very few organisations usually are also utilising computers even if it be not theirs.

The imminent need to maintain the integrity of data processed by the computers needs to be over-emphasised. While controlled use of computers by management is an aid uncontrolled use of computers will and does have adverse impact on the organisations. This would result in inaccurate and incomplete information forming the basis for decision making.

It is in this background that one has to become aware of the need to have controls in the usage of computers. With the extensive technological developments in the hardware and the sophisticated techniques in the development of software, the norms of controls necessarily keep changing.

As it is the primary responsibility of senior management to ensure that necessary controls are in place, they look up to auditors. Auditors have a responsibility to discharge their duty and maintain professional standards. With
varying types of computer environments, there are appropriate control procedures to ensure that the data is processed correctly and completely.

Nature of the problem

First of the generally accepted auditing standards issued by the American Institute of Certified Public Accountants states that examination of books of an organisation is to be performed by persons having adequate technical training and proficiency as an auditor. The second standard of a CPA field work specifies as follows: "A sufficient understanding of the internal control structure is to be obtained to plan the audit and to determine the nature, timing and extent of tests to be verified".

The Statement of Audit Standards (SAS) further expects the auditor "To consider... complexity and sophistication of the entities operations and systems including whether the method of controlling data processing is based on manual procedures. As the entities operations and systems become more complex and sophisticated, it may be necessary to devote more attention to internal control structure and elements to obtain the proper understanding so as to facilitate designing effective substantive tests.

It further specifies that the auditor should obtain sufficient knowledge of the accounting system to understand... the Accounting process involved from the initiation of transaction to its inclusion in the financial statement including how the computer is used to process data.
The need for technical expertise on the part of the auditor is due to the impact of electronic data processing (computerisation of data).

The objectives of audit have not changed. It is only the means of achieving these objectives that have changed.

With the technological developments, there have been changes in hardware and software. Consequently control concepts have necessarily changed. Hence audit approaches also need to change.

HARDWARE

Hardware have come a long way from unit record equipments. The first generation computers characterised by vaccum tubes gave place to second and third generation computers which utilised transistors and integrated circuits. Subsequently, the fourth and fifth generation computers with more complex and sophisticated peripherals have appeared on the same.

These changes in hardware brought, in their wake, the disappearance of "Audit trails". It is the audit trail which enables the auditor to trace a transaction from a source document to a report or a total produced by the computer. The same audit trail also enables the auditor to reverse the process and be able to find out the source background or other basic information which have figured in the final report or total. Computers with multi-programming or multi-processing facilities have come into the picture. With these concepts, it is possible to have a number of programs working simultaneously or a single program to be processing different files simultaneously.
On-line and real time systems have much used facilities. These facilitate processing of data by transmitting them over communication lines. It is possible now for data being entered at one terminal, processed at other terminal and the results being made available at a third terminal. Real time systems enable updation of data immediately in as much as querying and obtaining of such information instantaneously is possible. Eg. Bookings of air tickets from anyone office from any of the many flights on different routes also on different dates.

Along with the advancement of technology in the field of main frame computers, there have been advances in the development of small and smaller computers. The advent of small and smaller computers have been creating big and bigger problems from the auditor's point of view. The auditor is not assured of certain basic controls which he is assured of in a main-frame computer environment.

SOFTWARE

Software consists of programs as distinct from hardware. These programs may be written by programmers within the organisation or may be bought out from vendors of software packages. Rigorous discipline is needed in the development of software before it can be permitted to "Go live". Auditors need to firstly be aware of the associated discipline with regard to the development of software and secondly possess the knowledge to evaluate whether the discipline is being observed or not. Thirdly and most importantly he should be in a position to assess the possible risks and loss due to non-conformity of the discipline.
Operating systems are also programs but they are special type of programs that are capable of managing and supervising the activities associated with the computer system. They handle all input, output operations, schedule jobs, allocate memory space etc. Operating systems while conferring a great deal of benefits are also a cause for concern. Many weaknesses in the operating system can cause havoc in the controls that are associated with computer applications.

DATA BASE MANAGEMENT SYSTEMS

DBMS reduces redundancy of data submission. It links various files and controls all of them. With the advantages of DBMS there are certain audit concerns regarding maintaining reliability and integrity of the different files in the DBMS. In view of the difficulty of tracing the transactions forwards and backwards, the auditor must have the capacity to test the integrity of the DBMS package.

LOCATION OF THE COMPUTER CENTRE

The practice of installing computers for performing accounting applications primarily and subsequently developing other incidental applications was the cause for the computer coming under the purview of the financial department. The Financial Controller generally was the administrative head for the Data Processing Department. With the awareness created for computer usage and the eagerness of the user department to develop their own applications the concept of "End User Computing" has come into existence. The controls that go with multiple terminals, multiple users, multiple system groups have a multi dimensional aspect and impact.
AUDIT

Ignoring the computer and treating it as a black box is no longer valid. An auditor cannot effectively function by auditing around the computer and auditing has come of age. Auditor has to audit thro' the computer "if not with the computer". While auditing, through the computer, auditor tests the client's computer programs by providing his own data and analysing the results.

While performing auditing with the computer, the auditor has his own generalised audit software which performs the audit functions on the computer system. Computerisation is taking place utilising to full advantage the latest technological developments. It is presumed that the controls that are necessarily associated with each type of environment are built into the system. An auditor, who has professional responsibility of giving his opinion on the statements audited by him, should possess adequate skills and capabilities to do so irrespective of statements and standards being pronounced by professional bodies or not.

DISASTER RECOVER PLANNING OR CONTINGENCY PLANNING

A fire accident which would char the edge of a leather-bound ledger is adequate to bring down an entire computer installation. Organisations are no longer mere users of computers. They are depending on them for their present existence and their survival in the future. Natural calamities like fire, floods, and other catastrophies, magnetic fields, viruses and intentional sabotages from insiders and outsiders of the organisation are dangers to be safeguarded against. Specific procedures need to be followed by organisations.
It is necessary to have an elaborate workable disaster recovery plan so that while all preventive steps would be taken to prevent a disaster, there should be a plan to recover from the disaster, well within the critical period, should it occur.

While furnitures and fixtures would be insured and the auditor checks the validity of the insurance policy, there is generally no such procedure being adopted with regard to computers. Computers are at the most insured for their actual cost. There has been no policy consi-dered to cover the cost of developing the programs, cost of re-creating the data as also consequential loss to the business.

The literature in the field of EDP audit and control is very extensive. Computerisation having been introduced in the developed countries like USA, UK, Australia for more than five decades, the awareness for controls and the need for specific audit evaluating the adequacy or otherwise of controls in particular environment has been in existence. Along with development of technology the controls have changed and necessarily the auditors have to keep pace with the same.

**SURVEY OF LITERATURE**

Over 50 publications, mainly from U.S., U.K., Australia have been studied and about 25 have been reviewed. From the extent of survey conducted, surprisingly, it is found that there has been no publication yet in India. This may be due to the fact that computerisation in our country has not been as long as in other countries to have reported cases of fraud!
None of the professional bodies in India seem to have even issued any Standards or statements as revealed by a review of the standards issued by the professional bodies in India.

A practice manual by Brian Jenkins and Anthony Pinkney provides a practical approach to an auditor for expressing an audit opinion on the financial statement of companies where preparation of accounting information has been computerised. Being a publication of a professional body, it is of particular relevance to practising accountants who are performing audits in a computerised environment. The principal objective of an audit is to ascertain whether in his opinion the financial statements on which he is reporting show a true and fair view of the state of affairs. It is of importance to note the principal features of the audit approach as mentioned by the auditors. The features mentioned are:

i) Each task undertaken by an auditor is a necessary part of the total work leading up to his report on the financial statement. Thus, the auditor has to concentrate his efforts in identifying these activities which would impact the truth and fairness of the financial statements.

ii) All stages in the audit are related to each other. Thus, the audit work and evaluation on controls is very closely related to the validation or verification of the financial statements.

iii) The approach is designed to provide alternative audit procedures so as to enable most efficient audit in particular circumstances.

---

(iv) The approach and documentation are developed internationally. However, the statutory requirements and policies are based on U.K. law.

The legal procedures and other statutory requirements are not relevant to our country. However, the fact that the auditor should understand the accounting system and evaluate the system of internal control and carry out functional test to satisfy himself with the controls are in place and working the way they should. This approach is the same whether it is a computer system or a non-computer system. Great emphasis is laid on understanding and recording the system. This book also recognises the usage of flow charts and/or narrative notes.

While discussing Audit approach for evaluation of internal controls the auditor emphasises the fact that for an effective evaluation it is first necessary to understand the nature of controls in a computer system. The auditor is expected to be conversant with "user controls, programmed procedures and integrity control". Programmed procedures include process controls, while integrity controls are controls over programs and files. They deal with implementation procedures, program security, computer operations and data file security controls. As a means to evaluate controls, it is suggested that an internal control questionnaire based on control objectives be prepared and necessary information gathered. It is emphasised control objectives do not change in any environment. The means of achieving these objectives differ depending upon the environment.

Chapter IV has a detailed discussion on control program procedure. These procedures ensure that only valid transactions are processed and recorded completely and accurately.
Chapter V and VI deal with integrity controls and their evaluation. The integrity controls are divided into

(a) Implementation controls
(b) Program security controls
(c) Computer operation controls
(d) Data file security controls and
(e) System software

Implementation controls deal with adequacy of procedures for the programs expected to be implemented. This may consist of new programs and include systems being developed or existing systems and programs being changed. The more important of the procedures while implementing a new system are

(a) System design and program preparation
(b) Program and system testing
(c) Cataloguing

Cataloguing is defined as procedures associated with making the "test programs" into "live programs". Cataloguing will include both manual and software procedures. The concept of programmed security controls is discussed. These controls ensure that unauthorised changes are not made to the production programs. This is of particular importance to the auditor, as an unauthorised change may be made by an individual so that he would benefit from the same. Example - receipt of increased wages, excess drawal from his account balance.
While dealing with compliance test which is referred to as functional test - an exhaustive tabular statement illustrating a specimen test corresponding to the nature of control is provided.

The Chapter "Audit Responsibility to internal control weakness" is of particular importance. The initial step in the audit approach is that the auditor should be able to identify internal control weakness, if any, and thereafter, assess the impact of such a weakness on the financial statement. He has to assess the materiality of such a weakness. Should the auditor decide based upon his assessment of the weakness that a material error could occur, he should take such steps as to satisfy himself whether such an error has arisen and if it has arisen, the extent of the same.

This publication of the Institute of Chartered Accountants of England and Wales drives home the point that a professional body has recognised the need for a different approach to audit in a computerised environment as distinct from a manual system. In view of the book having been published as early as in 1978, technology wise it is not upto date. However, it is of relevance to note that the professional body has deemed it necessary to publish a book of this nature to create an awareness and provide guidance to the Members of the Institute.

Objectives of Auditing in EDP environment\(^1\) have been laid down as follows:-

(i) To guide CPAs in auditing business enterprises which use computers for record keeping.

\(^1\) Gordon B. Davis "Auditing & EDP", New York, American Institute of Certified Public Accountants, 1968.
(ii) To provide a starting point for building a consensus of expert opinion on an auditing practices for examining such companies.

(iii) To suggest utility and applicability of different auditing methods where experience is still lacking.

(iv) To provide source materials for training and informational purpose. It is of great importance to note that this publication is dated as early as 1968.

Specific mention is made of the fact that EDP does not lessen the need for an evaluation of the system of internal control. On the contrary, it appears that increased emphasis must be given in the review of internal control to ascertain that it is effective. It is pertinent to quote that it is stated as early as in 1968: "Computers have been commercially available for fifteen years and the recency of the major impact can be appreciated by noting that it made in 1967 every use of all computers had been done in the preceding year, the number was expected to double again in the succeeding three years."

This statement is very relevant to the fact that though the computers have been in existence in our country for more than 40 years in some form or the other, technological developments and usage of computers in the last ten years have more than doubled compared to that in the previous three decades. The technology referred to in the book though out-dated, the concepts are of great relevance. The input processing and output controls are discussed at great length.

In view of the technological importance in the computer medium, some of the concepts on hardware are not of relevance. However, presentation regarding the programmed control over processing, evaluation of internal control and safeguarding
of records and files is of current relevance. There is reference to three methods of auditing viz.

(a) Auditing without computer
(b) Auditing through the computer
(c) Auditing with the computer

In the current context of technological developments, auditing without the computer has no relevance. It is more appropriate to audit with the computer. In the absence of such skill and competence auditing through the computer may be acceptable standard for effective auditing.

The questionnaire for evaluation of internal control is divided into the following significant paragraphs, each paragraph having useful questions.

(a) Background
(b) Organisation
(c) Control function
(d) Control over consol
(e) Management practices
(f) Documentation
(h) Program revisions
(i) Hardware controls
(j) Control over input and output data
(k) Process control relevant to each application
(l) Control over error investigation
(m) Physical safeguards over files
(n) Procedural controls for safeguarding files
(o) Capability for file reconstruction.

The questionnaire provides more than a starting point for the auditor who wishes to make a beginning.

The questions are numbered as A, B, or C according to the general control significance.

A - representing control element which may affect the auditor's evaluation of internal control

B - Control element which tends to affect data processing safeguards, but is however not likely to affect the audit procedures

C - Application affecting operational effectiveness or efficiency. ¹Elise G. Jancura and Robert Boos dealt with
  * Controls in system design and development
  * Controls in distributed and integrated system.

A detailed flow chart specifying the operation, the designation of the person performing the operation and the process are explained in depth. Though the narration is cumbersome, splitting up of the entire operations into various ingredients and connecting each step to the main flow chart is useful. The chapter on computer assisted auditing techniques deals with test data method, parallel simulation and usage of other programs written for a specific purpose or generalised audit software.

While this book makes an attempt in emphasising the need for establishing controls and auditing computerised accounting system, it does not specifically highlight the methodology to be adopted by EDP auditors.

W. Thomas Porter and William E. Perry have discussed the impact of EDP on auditing and control. They have discussed the concept of information as distinct from data. They have brought out the fact that one of the most difficult tasks an auditor has to perform while auditing is comprehending the systems. Flow charting is one of the very valuable tools that help the explanation of a system function. The concept of flow charting with detailed instructions and illustrations is well brought out. There is the problem of timeliness. There are tendencies very often to modify the system without updating appropriate flow charts. This problem could be got over by utilising the facilities provided in the automatic flow-charting systems. Flow charts of a programme could be obtained from the Source Code Statement. A specific mention is made of 'HIPO' - (Hierarchy plus Input, Process, Output) is a documentation aid. It has the ability not only to document the functions but also to show the hierarchical inter-relationships between these two functions. This aspect is extremely useful to the auditor. The subsequent chapters deal with controls in EDP system under two categories:

(a) General and administrative controls
(b) Application controls

Every system is liable to have an exposure. Exposures or risks are threats to a system. Controls are a means to reduce these risks. In a computerised system, there

---

is concentration of duties and functions which leads to certain complexity. Hence
there are greater potential for control problems.¹

Administrative controls deal with policies and procedures. They cross
application boundaries in view of the centralisation of the data processing activities.
There is concentration of many processing steps. In view of this, there needs to be
segregation of duties specially in incompatible functions like programming and
operation. A useful checklist for organisational control is provided. Organisation of
EDP department is of utmost importance and special attention should be paid to the
following:

(a) System and programming of controls
(b) Review and approval of new systems
(c) Programming-testing procedures
(d) Programming-change procedures
(e) Documentation standards

These would ensure a high degree of processing reliability. There should be
standards established for operating practices. They should include

(a) Access to computer room
(b) Library and file control standards
(c) Data conversion standards
(d) Physical security of files and equipment (e) Back-up facilities
(f) Passwords.

¹ W Thomas Porter and William E. Perry "EDP Controls and Auditing" - Third
Interesting problem of a live case has been presented. It deals with Equity Funding, insurance fraud.

Application controls are designed to meet the specific control requirements of each processing application. The controls are classified as preventive, detective and corrective controls. Preventive controls are controls which stop problems from occurring and expected to help "things happen as they should". Preventive controls are located throughout the entire EDP System. These are executed before the data enters the system.

The more important of preventive controls as discussed are

(a) Source data authorisation
(b) Data conversion
(c) Turn around documents
(d) Pre-numbered forms
(e) Input validation
(f) Controls over processing

Detective controls are expected to bring potential problems to the attention of individuals for appropriate action. Examples of detective controls are

(a) Control Register
(b) Control totals
(c) Documentation and testing
(d) Labels
(e) Output

---

Corrective controls arise in the investigation and correction of cause of exposures which have been detected. Typical examples of corrective controls are

(a) Audit trails
(b) Discrepancy reports
(c) Back up and
(d) Recovery

While discussing on Review and evaluation of controls in EDP Audit system, it is recommended that understanding and testing of the system should be achieved through an analysis of the client’s entire system of internal control. Once review and testing is over, it is possible to evaluate the adequacy or otherwise of the control system and make recommendations if any. There is an interesting case study provided with a useful questionnaire with hypothetical answers.

The audit approach when the client’s use service centre is different from usage of a computer in-house. The audit approach when the client uses a service centre is discussed.\footnote{W.Thomas Porter and William E. Perry "EDP Controls and Auditing" - Third edition, Massachusetts, Kent Publishing Company, Boston, 1981.} A specific mention is made of advanced auditing techniques including test audit method, test case, system evaluation, integrity, test facility and parallel simulation. It is very well brought out that in an environment of accelerated changes in computer technology, newer and up to date auditing techniques are needed.
S.Rao Vallabhaneni, traces the importance of software in a computerised environment. He mentions that 50 to 75% of the time of the system analysts and programmers is spent in maintaining the existing software and that more than 50% of the operating budget is for software. He brings out the fact that inspite of the above mentioned significant facts, auditors do not spend enough time reviewing, testing and evaluating the controls in the application systems when they are in the process of being developed. He correctly mentions that more time is spent on software development activities than for reviewing software maintenance controls. He explains the difficulties faced by systems and programming staff who are under pressure from the users and suffer from lack of appreciation of concepts by senior management. Many a time software is developed without considering future maintenance. Very few programs and systems are developed using structured techniques. This results in great deal of patch work being done. He refers to "spaghetti code" which is difficult to control, maintain, modify or audit. In view of the absence of usage of structured techniques the systems staff are constrained to use an adhoc approach.

Maintaining software is a human activity which is error-prone and has a high risk. Unless documentation is adequate a previously bug-free program may land up with problems unless the modified program is thoroughly tested.

The emphasis of this book is to highlight the importance of software maintenance activities along with their associated risks and exposures and to provide guidance to auditors for evolving procedures and approaches. The focus of the book

---

is on the Internal Auditor and makes reference to SAS No.9, issued by the American
Institute of Certified Public Accountants - the independent external auditor should
consider the procedures if any performed by the internal auditors in determining the
nature, timing and extent of his own auditing procedures".

Thus, it naturally follows that if the internal audit's review of software
maintenance is more comprehensive, the external auditor's scope should be less
comprehensive. The term software maintenance is used to describe all changes made
to a computer program after it has been implemented in a live environment. He
refers to US General Accounting Officer (GAO) Report - Page 5, footnote :

The GAO studied 15 computer sites in detail and received responses for
mailed questionnaires from several hundreds. It is mentioned that though the study
was relating to Government environment, it is equally applicable to private and public
sectors. Some of the problems enumerated are:

(i) Software maintenance cells are not easily identifiable
(ii) Expert user requested modifications are not always based on real need
(iii) User requirements in the software development phase are not adequately
defined.
(iv) Application systems document is inadequate if not missing.
(v) Computer programmer's attitude towards software maintenance is not
enthusiastic.

These points are of relevance to the environment in our country also. The
time and effort spent on system development phase is not always productive either
because users do not define their requirements precisely or the systems staff decide
on their own on certain requirements of the users. As most of the applications are to be modified under pressure, documentation procedures are given the go by Priority is for keeping the system going with the modification. In the circumstances, the capacity of the auditor to understand the modification and evaluate the controls needs special mention.

The author has divided the book into three parts, the first part dealing with environment, the second part with control guidelines and the third one with audit methodology; the fourth one being on viewing the future. He explains the software maintenance life cycles (SMLC) as distinct from SDLC by dividing the methodology into different phases. For each of the phases, he lays down the objectives and activities and from the auditor's point of view, the final deliverables for control review and final evaluation. He highlights the point that auditors, specially the internal auditors with resources use for software maintenance are adequate and that they are used effectively and efficiently. He highlights in chapter IV that the auditor needs to be aware of what can go wrong in software maintenance, he highlights three types of control, viz. preventive, detective and corrective which could prevent irregularities and omissions during software maintenance. He provides a table of audit tools and techniques - use matrix.

The book is an excellent treatise of the procedure to be followed in an ideal situation. While it may not be possible to give an ideal, a reading of the book by an auditor creates an awareness of the reality of the problem and possible practical steps he should take to ensure adequate controls are introduced in the software maintenance phases.
Technology is advancing important supportive functions that protect the technology from intentional losses is not keeping pace. He makes reference to the systems auditability and control reports produced by Stanford Research Institute International of 1977 and observes that auditing which is an important supportive function is lagging far behind. In view of the auditors lack of sufficient knowledge of the technology, he is constrained to rely on the trustworthiness of computers, computer programmers, operators and other computer staff. An auditor is expected to be independent in attitude and appearance and the dependence of the auditor on data processing staff is violative of basic audit principle. The author has very relevantly mentioned that the auditors performing their function in a computerised environment have realised that they have to acquire necessary skills to perform their jobs competently. Similarly, data processing management are realising the need and value of the services of the auditors who evaluate the adequacy of controls in the computerised environment. The book which has the focus on creating an awareness in the management of organisations which have introduced computers deals with the subject in a non-technical manner. The authors make special reference to transmittal memorandum 1 circular A/71 on security of federal automated information systems issued by the US office of management. This memorandum establishes a comprehensive policy regarding establishment of computer security programmes in all non-defence computer centres also. The objective is to establish of procedures for adopting security standards, a requirement for security in all hardware and software procurements, guidance on conducting risk analysis, performing security audits, developing contingency plans and establishing personnel security policies.

This memorandum is considered a mile-stone for computer security even as early as 1978. One whole section is devoted to the nature of computer security. A useful table giving details of various types of security areas to be safeguarded and how it could be safeguarded are explained lucidly. Concepts of risks and threats are explained. The author is of the opinion that what may appear as accidental and unintentional acts may not in reality be so. He drives home the point that one should be prepared for the worst and provide adequate security functions. While discussing the aspect of deterrence which would be a preventive measure for the likelihood of security violations, the author makes special reference to audit. He very pertinently points out "one of the greatest values of auditing is deterrence". The aspects of preventive, detective, recovery and corrective controls are discussed with effectiveness. The importance of contingency and back up plans is discussed in detail. While discussing the recovery issues, the factors to be taken particular care of are mentioned as

(a) Staffing : the safety of people is of primary concern
(b) Facilities and neighbouring site : considering the risk factors in the neighbourhood of computer room is of immense importance.
(c) Utilities : automatic local telephone switching centres or automative underground cables would affect on-line systems. These need to be protected to the same extent as computer or power supply or air-conditioning equipment. Other important factors like documentation standards, storing of production programs, operation system utilities, and data in a place away from the main operation which are mentioned are helpful. The book deals also with security factors for a computer site selection.
The aspect of earthquake which seems a theoretical concept in our country has been considered as a possible reality by the author and guidance provided. Suggestion regarding consulting geologists are made.


Section 3 of the book deals with computer security program and deals in great detail on the following subjects.

(i) Identification and valuation of assets
(ii) Identification of threats and risk assessment

While dealing with safeguards, *special mention is made of auditability*. It mentions that safeguards must be testable for the purpose of auditing its performance and compliance with specifications. While illustrating this point, an example is given of an auditor visiting a data processing facility and asking to be shown recovery from remote back-up files. The EDP department sent a vehicle to collect the back-up files, programs and operating instructions. It is interestingly reported that at this point, the test was terminated because if all the back up materials were returned to the computer centre, there will be no back up material at the remote site. This lead to the organisation having two copies at the back-up site.

While concluding that EDP auditing is an important activity for computer security, it is mentioned that auditing tools and techniques must be considered as one of the most important safeguards. An interesting matrix on EDP audit tools by occupation applicability is revealing.
"Micro computer security, auditability and controls" deals with the subject in three parts.

1. Microcomputers in general
2. Stand-alone microcomputer systems and
3. Micros connected to mainframe systems.

In Part I while dealing generally with micro computers, the book provides statistics from a report regarding the growth of micro computers. He quotes the market has gone from US $200 million in sales to a projected 426 billion dollars in sales in 1983. In 1983 about one million units were sold and it is expected that 45 million units may be sold by 1986 or 1987.

A tabular statement providing the prevailing characteristics and associated threats are illustrated. Among the prevailing characteristics the following are mentioned:

* Proliferation of application development
* Staff limitation
* Applications software
* Hardware
* Vendor system software, standards and practices
* Physical environments, file and media storage outside
* Unauthorised access.

---

Under each of these heads, the conditions that are prevalent in a microcomputer environment are discussed with the associated threat. A detailed reading of the above threats focuses attention on the fact that there is a clear need to have a well formulated set of control objectives with effective safeguards which provides solutions for a secure use of the microcomputers.

Chapter 3 of the book deals with auditability considerations. A useful table giving the prevailing condition and the corresponding auditing concerns and considerations is provided. To sum up, the problem generally faced by auditors are

(1) When same application is processed on different computers, how is the integrity of the application to be decided unless all the units are audited.

(2) With paucity of staff, there is no separation of duties.

(3) Audit trails may be lacking in view of lack of facility for logging. When software packages are developed lack of documentation exists. Information regarding what types of error handling and controls are included is not easily available. The author proceeds to deal with the control system dividing it into three zones as follows:

(1) General and administrative controls

(2) Micro computer system

(3) Micro computer software

While dealing with connected micro systems he deals under three zones as follows:

(a) Data communication

(b) Micro computer

(c) Mainframe penetration by Hacking
The fact that security and protection of micro computers is as important if not more important as the security of log system is emphasised. While dealing with general aspects of micro computer security, software and data integrity issues of concern are mentioned as follows:-

- Who can access the micros
- To what extent can they access
- How is the data protected from the unauthorised distribution
- What is the possibility of loss of critical data
- How is data integrity to be maintained
- What is the possibility of intrusion from outsiders.
- What steps are to be taken for maintaining continuity of operations.

The book provides

1. sound framework for dealing with internal and security controls
2. An overall coverage of security auditability and controls
3. A complete set of management policies and standards for management control of this new technology
4. A comprehensive list of control objectives, control techniques for different types of micro computers.

A set of specific objectives along with a list of specific control techniques which would meet the control objective are mentioned.¹

The author discusses as to what kind of control the designer and the auditor should consider to build security and integrity in the advanced on line systems. He also deals with audit approaches and techniques which would effectively and efficiently audit and review the systems. A tabular statement distinguishing the various features of the systems with the respective implications of such a feature are well brought out. While dealing with internal controls, the author classifies integrity under four categories:

(i) Accuracy  
(ii) Security/privacy  
(iii) Continuity  
(iv) Environment  

The author divides the control zones under 8 heads:

(i) Data entry 
(ii) Data communication 
(iii) Systems environment in general controls 
(iv) On line application programs 
(v) Data base 
(vi) Data base administration 
(vii) Environmental software 
(viii) Data base control zones and audit base development standards  

Under each of these heads, the author deals with the following:

(i) General control objectives  
(ii) Various control points
Under each of the control points, the control objective and the corresponding control techniques are discussed in detail. The two parts of the book contain a precise presentation of the entire subject.

Computer Security

Keith Hearnden\(^1\) presents a collection of 14 articles on computer crime and people, computer crime in the 1980s, risk management and computer security. While all the articles have special reference to the accepted procedures for security maintenance, there is narration of live cases of crimes committed on computer. The importance of these article is that computer crimes and frauds are not academic issues, but are realities which have been perpetrated in most cases by computer literates. This has been possible by penetrating the vulnerable points in the control systems of computers.

Security is the integral part of the design and implementation of an information system. V.P.Lane\(^2\) interestingly brings out the fact because that in many instances security involves cost, the decision of the management may be to ignore certain security requirements, considering only the cost factor, He highlights the fact that good security must be built into the system software before individual applications are designed. He deals with physical security and data security. While discussing physical security, he classified it under two major heads viz.(1) protection

---


against natural disasters like flood and fire (2) protection against intruders. Under the head natural disasters, he places special importance to fire and discusses at length the advantages and disadvantages of carbon-di-oxide as against Halon and water sprinklers.

While discussing access control and intruders, he highlights three ways of controlling access.

(i) By using receptionist and security officers
(ii) By using mechanical devices such as locks and keys
(iii) Electronic systems using identity cards/card readers

A systematic approach is necessary if a realistic plan for physical security has to be evolved. The author stresses the view that the management must assess what they are trying to prevent and protect. To achieve this, he suggests the following should be performed:

(i) Identify undesirable events
(ii) Evaluate physical threats and the probability of such an event occurring
(iii) Estimate possible loss to which the computer/premises are exposed.
(iv) The expected annual loss.

While discussing data security, it is stated that it could be maintained by four kinds of control viz.

(a) Access
(b) Information flow
(c) Inference
(d) Cryptographic controls.
The author stresses the point that while these methods can reduce danger of compromise of data, they cannot totally eliminate the possibility. The security role of components of computer configurations is highlighted by each of the aspects of hardware, systems software etc. While discussing the system software i.e. the operating system, its security functions are classified under two heads viz. Implicit security function and Explicit security functions. Under Implicit security functions are included those security features that manage and control the system resources and application programs. The explicit function include surveillance and identification, access control and isolation. The chapter dealing with people and security highlights the fact that sometimes the position of power exercised by a single individual like system administrator is both a weakness and a strength. He suggests remedial measures as

(i) Job rotation
(ii) Supervision by a superior
(iii) Journalising i.e. recording request from the administrator or log to facilitate auditing and examine the log for unauthorised activities.

Security aspects of the operation of computer facilities include training of computer operators, library management system as also short term recovery procedures. It is emphasised that management must highlight the fact that security is needed even during routine operating of the system, to make the effort of planning overall security aspects a success. Special topics like privacy and data protection legislation and protection of proprietary software are discussed. The author concludes that software is currency; It is essential that those who provide the currency are protected from counterfeiting and duplicity.
Chapter 11 of the book deals with a number of real life incidents. Amongst more interesting cases are that of a supervisor of a payments department in a local authority in London. He found a method of creating false documents. This resulted in a loss of approximately 40,000 pounds. Yet another case deals with how an executive officer utilised the computerised salary system to defraud health authority. A novel, yet a case of great concern is where computer personnel stole the computer files and demanded ransom for restoring them. Fortunately, the culprits were caught. The last case reported is regarding a boiler explosion which destroyed the computer office site. The author concludes that the misfortune did not become a calamity because of the contingency plans of the company. The 1981 survey and the 1984 survey regarding incidents involving theft and misuse are very revealing.

James Arlin Cooper¹ discusses early development and environmental aspects under the following heads:

* Physical security
* Personnel security
* Regulatory security
* Hardware security
* Software network security.

Each of these environments are discussed in great detail under various heads of prevention, detention and correction. It is of importance to note that a mention is made of the computer Act of 1987. The Act requires the establishment of security

---

standards for Civilian agency computers and communication systems. The author makes a comparative study of the regulatory requirements in different countries like UK, Canada, France and Sweden. A reading of these legislations and their development makes one realise that other countries from their experience have found that legislations are necessary which makes us to think that in view of the wide computerisation, it would not be too long before our country also feels the need. While discussing the software security environment, the author highlights the fact that the verification of system security features and system security performance can best be achieved only by EDP auditor function. In the author’s words,"EDP audit, if properly done, gives additional insight, identify signals that point out security, weaknesses or failures and helps prevent security by-passes resulting from collusion." He even goes to the extent of mentioning that a 30 million fraud which he discusses in his book was possible because audit procedures were relaxed. He discusses amongst others 14 tools and techniques and concludes that audit procedures give a degree of protection against intentional attacks. They make a perpetrator’s job difficult as the chances of detection are high. While discussing the current perspectives of computer security, he highlights the security strength by discussing the encryption techniques and also does not lose sight of the negative side of the security i.e. weakness. The problems of controlling access uniformly and reliably over widely dispersed locations is difficult. The author discusses the research perpsectives of the 1990s as also the outlook for the 1991s.
DISASTER RECOVERY PLANNING

The need for planning for disaster recovery in a computerised environment is explained.¹ The three areas of exposure that the management needs to review as described by the author are financial loss, legal responsibility and business interruption.

Part I deals with management considerations. A detailed questionnaire deals with disaster recovery priority concerns of management under the heads:

1. Staff protection and actions
2. Maintenance of customer services and
3. Cash flow maintenance.
4. Vital documents protection
5. Facilities equipments,
6. Programs and
7. Supplies.

A reference is made to three levels of security and disaster recovery measures viz. mandatory measures, necessary measures and desirable.

Mandatory measures are those needed by law. Necessary measures are those reasonable precautions which need to be taken.

The desirable measures although necessary are not needed to be implemented as immediately as mandatory measures. Desirable measures are implemented as and

when circumstances permit. A cost benefit analysis is made taking into consideration the perceived and desirable needs.

The second part deals with conducting the review programme. It is considered necessary to establish disaster recovery review objectives. The first and foremost, the types of disaster need to be identified followed by identifying the areas which may be impacted by a disaster. It is necessary to review the disaster recovery controls. A useful workshop concerning internal back up site, checklist is very educative. A specimen typical agreement with time brokers viz. those who would find another site that a company can use in the event of a disaster is informative. The author gives procedure for testing the disaster recovery programme and classifies the testing into, static testing and dynamic testing. He deals with different techniques for testing and gives the base for selecting the appropriate technique. The basis for evaluating the basis for disaster recovery test are discussed. The important aspect regarding insurance coverage is highlighted. The fact that extra insurance is needed on back up site is also mentioned. The principle of insurance coverage, as is wellknown, is to transfer the risk of major loss to another organisation. There should be a competent person for deciding the degree of risk to be insured. It is recommended that the cover should be for each class of equipment, records, media, mentioning their replacement costs and actual cash value. The points to be considered while discussing with the insurance manager include also extra emergency expense, third party liability, revenue bearing data. The extra emergency expenses include rental of temporary facilities, back-up equipment, moving cost, temporary insurance cost. The third party liability arises only in the case of service bureaus. The example of revenue bearing data would be the data regarding the outstanding balances. Following the testing of
the disaster recovery program would be the procedure to evaluate the DRP. Various concerns and opinions regarding the adequacy of the disaster recovery programme need to be formed. This opinion is to be supported by sufficient evidence collected during the review process. It is necessary to evaluate each concern individually and then the totality of the individual evaluations should be reviewed in making a final judgment. A useful guideline regarding writing disaster report is provided. It is recommended that it should have the following chapters:-

(i) Management summary
(ii) Scope of review
(iii) Background
(iv) Findings
(v) Opinion
(vi) Its impact of opinion
(vii) Recommendation.

Robert R. Moeller\(^1\) deals with computer audit, control and security aspects in a computerised environment and the appropriate audit methodology. The controls are considered under the following three environments \(viz.\)

(1) large computer centre,
(2) mini micro computer centres and
(3) distributed network.

In Section 2, he deals with auditing data processing applications. He deals with the methodology to be observed in selecting applications for review. He describes the

procedures to be followed. Different testing techniques and methods of evidence gathering in a paperless environment are discussed. The author emphasises the need for the auditor's role in reviewing new applications and their development.

In Section 3 he emphasises the need for

(a) physical security
(b) information security and integrity and
(c) an effective disaster recovery plan.

There is a special chapter on audit and control of end-user computing. The many forms of end-user computing, the controls associated with end-user computing are discussed. The author provides a list of control objectives and procedures for reviewing various controls. The tabular statements are extremely useful and are in detail. The auditor can make a ready reference to anyone situation in which he may be placed and immediately have an exhaustive checklist. The author has provided this information also on a diskette. This can be used on an IBM PC. This enables the auditor to carry the floppy and have a ready reference to the list immediately in any of the client's offices. The author discusses the successful modern internal audit function. He is of the view that an audit professional of the future would have to have strengths in financial, operational and computer auditing. He concedes that while it is an ideal situation, an individual who possess all the qualifications may not be immediately available. His remarks are very significant. His description represents the audit of the future in the modern organisation and it should be an audit organisation's goal to build personnel with these skills. He adds, that there is continued need for special techniques for computer audit in view of the technical environment in the organisation. While describing the audit department of the future,
he states that "the computer auditor specialist of today who spends much time looking at the general controls within the computer operations area does not get into user areas to evolve application controls, and assess possible risks, runs the danger of becoming obsolete in the era of modern data processing procedure. The auditor should develop financial - or operational audit skills, as well as computer and audit skills to operate as the organisation's auditor of the future". This statement of the author takes into consideration that the present day auditor is able to evaluate the general controls!

It is of significance to note that in our country auditors are not even able to evaluate the general controls. In view of the wide gap of the expectation of the audit department of the future, in the present position in our country there needs to be realisation about training auditors to attain better skills and competence to really operate as organisation's auditors of the future.

William C. Mair, Donald R. Wood and Keagle W. Davis have made a very comprehensive presentation of the various aspects of auditing in a computerised environment. The matrix presentation is the highlight of the book. There are four matrixes as follows:

---

Application control evaluation table

It deals with application causes of exposures under the heads input, processing, output and others. For each of these causes, preventive, detective and corrective controls are considered.

Systems development control evaluation table

Under the causes of exposure, it deals with incomplete economic evaluation, management abdication, inadequate specifications, system design errors, incompetent personnel, unmanageable application etc. The controls again are classified under preventive, detective and corrective controls. The reliance on controls are classified as

(1) useful but not especially effective
(2) control cause but should be accompanied by additional controls
(3) Reliable controls

Computer abuse control evaluation table

The abuse is classified under object tool and environment and the controls again are classified as preventive detective and corrective.

The last table deals with information processing facility control evaluation. Causes of Information Processing Facility exposures are classified as human errors, hardware defects - software failures, computer abuse and catastrophe. The controls are classified under the heads preventive, detective and corrective. The authors have
achieved the objective of helping the auditors to understand as to what is meant by adequate control in data processing environment.

Mr. Per Brinch Hansen\(^1\) provides a overview of operating systems and gives a technical description thereafter of the various aspects of the operation system. Ignoring the technical content, it provides a good understanding of the concept of an operating system and its capabilities and how it works.

William E. Perry\(^2\) divides the auditing information system function into 30 tasks and classifies them under the following functions:

- Scoping the environment
- Understanding the information system
- Identifying the audit risk
- Identifying the audit evidences
- Identifying key control points
- Identifying control weaknesses
- Verifying the integrity of the computer files
- Conducting the audit and concluding the audit.

The relevant tasks under each of these functions are discussed in great detail. The author provides an approach for audit of information systems by concentrating on the business processing sections of information system. The analytical approach

---


is of immense use and this approach has been adopted by me in my questionnaire and discussion with the auditors.

S.Rao Vallabhaneni,\textsuperscript{1} while introducing the concept of software development process, presents both the management and the auditors concern over software. He discusses in detail the problems and issues that arise in development of application system whether it be developed in-house or by outsiders. He clarifies the responsibility of the senior management, data processing management and the end-user in relation to the software development problems and issues. The fact that the auditor especially the internal auditor has a specific responsibility with regard to the software development process is highlighted. The author discusses the audit strategies and the control guidelines. He discusses in detail the audit methodology in the following areas.

* Planning phase requirements,
* Design,
* Programming,
* Testing,
* Conversion,
* Post implementation.

He concludes that if an auditing is undertaken of the software development, the chances of its being usable, maintainable, auditable, controllable and securable are very high. The author discusses 15 case studies in different environments. Under each of these case studies, he describes the system audit scope and objectives and

finally mentions audit findings and recommendations. While summarising the findings of the 15 case studies, he concludes that knowledge of auditing software development when practiced properly would make organisations more aware of system integrity and security controls.

Michael A. Murphy and Xenia Ley Parker\(^1\) of Coopers Lybrand, International authorities on EDP Auditing deal with the impact of EDP on Auditing as also the information technology concepts. The entire book is written with the auditor in mind. Even technical aspects are discussed in great detail in a manner which can be understood by an auditor. In their chapter of information systems, they deal with business systems to enable the auditors as also the technical personnel to get an overview of a computer application systems. A special chapter deals with application controls. The authors deal with methods for documenting systems including usage of flow charts. While discussing audit of systems development, they highlight the practice and methodologies to be adopted. There is a special chapter on End-user computing. It is of immense importance to our current scenario with the proliferation of personal computers. The authors discuss the management risks and issues as also user control and risks. While discussing the applications of end-user’s, they make specific reference to usage of spreadsheets, and the associated risks and the specific controls to be used. The auditors’ role in end-user computing is discussed and a view is expressed that the auditor should evaluate the controls in the following risk areas:

- Software and data integrity
- Back-up and contingency planning

Auditability

Multi-user micro computer

Communication security

Controls in service bureau are also discussed. There is specific reference to third party review of service bureau. A detailed workplan along with a specimen of a summary and third party review of application and data centres is of immense use.

The chapter on testing techniques by computerised systems includes the topic on use of computer assisted audit techniques (CAAT).

The 1993 cumulative supplement deals with more current concepts like Expert Systems. While discussing the information technology, concepts, and meeting future needs the authors who have international reputation have stated as follows:-

"Future auditing impacts of new information technology is significantly altering the conduct of audits... At a string to the credibility of management assertions has been one of the provisions major responsibilities during its entire history. For years, the service has been epitomised by the annual audited financial statement. To-day, the annual financial statement - while still serving a valuable role by becoming a smaller part of the information needed by management.lenders and stock holders to make informed decisions... As other sources of information become more and more important, there is a current need to develop ways to similarly assure their currency completeness, neutrality, freedom from bias and credibility.

The challenge - and the opportunity for the public accounting profession is considerable. Professional standards will need to be developed to cover these possible
new services. In addition, the responsibility that public accountants would assume and
the legal exposures they would incur would need to be assessed. Most important,
however, there is a clear indication of need, and the profession is well situated to
respond".

It is important to note that the situation regarding technological developments
and usage of computers have changed in our country also. The profession in our
country is not well equipped to respond and the management of organisations are not
as yet ceased of the problem.

Research publications

The publication of the Institute of the Internal Auditors USA\(^1\) reviews, risk,
controls and audit techniques while describing the fast changing technology to help
internal auditors to perform their jobs better. The report consists of 11 modules as
follows :-

- Executive summary
- Audit and control environment
- Using information technology in audit
- Managing computer resources
- Managing information and development systems
- Business systems
- End-user - departmental systems
- Telecommunications Security

\(^1\) Price Waterhouse, "Systems Auditability and Control", The Institute of Internal
Contingency Planning

Emerging technologies

The project was financed by IBM and Price Water Hons performed the work. The report clearly recognises that the internal auditor's responsibility regarding information technology has changed tremendously. The report concludes that as a major aspect of strategy planning, the auditor should have an overall assessment of associated risks and concerns, to emphasise the fact that the auditors need to be current. It is necessary for the internal auditors to understand the environment and the technology, to enable them to inform the management correctly about the actual and potential risks and control concepts.

Mr. Kamal Gupta, Technical Director of the Institute of Chartered Institute of India while discussing various aspects of audit, devotes whole chapter on auditing EDP based accounts. A reference is made to the various standards and pronouncements of professional bodies abroad. It is recognised that the increasing use of computers has changed the approach and techniques of audit also. It is reliably learnt that in view of the increased use of computers, the Institute of Chartered Accountants itself has made a start in providing guidelines to its members for procedures to be followed while auditing in a computerised environment. It is learnt that the Indian Institute also may be within 2/3 years after the process of different committees, approving the same, is completed issue official professional standards as a statement hopefully.

Professional bodies elsewhere in the world, have issued standards for Auditing Practice in a computerised environment.

S.Rao Vallabhaneni\(^1\) discusses the audit methodology and control guidelines. He classifies the computer security under the following heads:-

- Physical security
- Personnel security
- Data security
- Application software security
- System software security
- Telecommunication security
- Computer operation security

While critically analysing the various concerns, he has prepared useful worksheets for risk assessments in the different areas. The criteria considered is very exhaustive and the methodology very practical. He has provided values for the risk and weightage for the criteria and arrived at the total risk score. He has a very useful suggestion of preparing a risk ranking worksheet which, from the data collected on each of the computer security areas, grades, the risk level as "low, medium and high". An analysis of this approach and his conclusions have a practical bearing. The methodology adopted for risk assessments for the purpose of my study are similar to the one proposed by this author. A copy of the questionnaire for risk assessment under each area of security and risk assessment worksheet are enclosed. (Ref. Appendix).

Watney and Peter\(^1\) deal with computer auditing as a conceptual foundation. The topic of internal control structure is presented under the heads of organisation controls, personnel practices, standard operating procedures as also systems development documentation controls. Specific mention is made to the systems documentation standards. The documentation is expected to have the following:

- Problem definition
- System documentation
- Program documentation
- Operations documentation
- User documentation

While conceding that maintaining good standards of documentation is necessary, the author realises the difficulties in maintaining the same. He makes specific reference to software aids to documentation. The section dealing with auditing EDP systems is of importance and the auditing is divided by authors into the following tasks:

- Audit of computer programs
- Audit of data files and data bases
- Audit of computer processing - general concepts
- Audit of computer processing - user control systems
- Audit of computer processing - third party systems

---

Mention is made to usage of expert systems and the role of auditor in auditing such an environment. It is interesting to note that the author mentions that the auditor should use the expert system as a tool to be more effective and efficient.

Ron Weber's book is a bible to auditors who wish to gain basic knowledge of computerised environment, associated controls, evidence collection methodologies, and evidence evaluation procedures. There are important chapters on managing EDP audit function. The author highlights the importance of changing EDP audit function. With the advent of micro computers, growth of end-user computing and impact of knowledge systems and the growth in data communications, the authors feel the EDP auditor should keep pace with the new technology. An interesting question posed by the author is as to how an auditor can determine what changes need to be made to controls and audit procedures when an organisation changes from its existing technology to new technology for its data processing. He concludes that the role of EDP auditor and basic audit methodologies remain unchanged. However, the EDP auditor must understand the new technologies, be capable of determining their impact on controls and audit procedures and ensure that appropriate evidence collection tools and techniques have been developed.

Michael G. Grottola elaborates on using UNIX to Audit Unix. He provides guidelines as to how the operating system UNIX can be controlled by its owners. His book deals with facts concerning what to look for in an UNIX system, how to


examine it and how to report its findings. The author mentions that using a UNIX operating system to audit the environment thus require apart from audit experience, UNIX literacy. It provides useful guidelines for the auditor to become "Unix Literate". There is a chapter on which it takes the auditor through the various process of installing the UNIX system. It gives a brief description of each of the commands. The book contains useful information on how an effective audit can be conducted in an UNIX environment using the UNIX commands themselves.

Unix Security is an important subject. Mr. N. Derek Arnold¹ while helping the reader to learn about the UNIX operating system, concepts and securities, also helps the understanding concepts of information control and security aspects. A special chapter on audit programs refer to the several ways the systems auditor can keep track of what is going on in the system. It highlights the fact that more the system administrator knows about the activities of the system, better steps can be taken to secure the system. The importance of End-user maintenance is highlighted. The possibility of new user's messing up needs to be borne in mind. The vulnerabilities because of installation of special devices are discussed. It is mentioned that devices which have the potential to bypass standard unix security are being built. On the face of it though the publication looks as if it is highly technical, it is of immense use to the auditor as it contains useful guideline for the usage of different commands. The ways of bypassing security by using yet other commands are highlighted. There are special chapters on data base security in unix environment. The chapter of "breaking techniques" is very revealing as it describes the method used by an attacker. As the author mentioned, this is of particular use to the administrator. The techniques

mentioned in the chapter are of immense importance, as the knowledge of the facts will help the auditor to know what could happen. Yet another chapter on VIRUS infection helps to get an understanding of how a virus works in a UNIX environment. This chapter provides some guidelines on how viruses can be prevented and if prevention fails how to detect them. The problems associated with prevention and detection discussed in this chapter gives an insight into the problem that one will face when a virus infiltrates in a computer system in a unix environment.

Database management system and system functions are explained lucidly by Gordon G. Everest. Specific chapters on data base integrity dealing with back up and recovery, quality control and concurrent update access control and encryption are of utmost importance to the auditor. The author explains in simple language the concepts of data base, provides guidelines for the auditor to acquire knowledge on the necessary controls in a data base environment. The awareness of the knowledge of the controls and the procedures which should be implemented in a data base system facilitates the auditor to test the adequacy of the controls in a data base management system environment.

The literature surveyed deals with different computer environment and the controls and audit concerns associated with it. Each of the technological developments have been dealt with in detail.

However, a concerted study of what the auditor is expected to do in a computerised environment as per the auditing standards of different professional

bodies taking into consideration control objectives and audit concerns in specific computerised environment, specially as prevalent in India, is not available.

The study has been undertaken to attempt to fill up this gap. A sample survey of control and audit practices has been undertaken and analysis included.

IMPORTANCE OF THE STUDY

The present study is an attempt at evaluating the controls in different computerised environments generally and specifically like End User Computing, networking, Data base management. A study of the controls that should exist in the different computerised environments has been made. This has been compared with the controls that are existing in a sample set of organisations in different environments. The audit concerns in each of the environments in particular and in a computerised environment generally has been stated. An analysis of the findings has been reported with suggestions, based on the findings.

A study of the professional statements and auditing standards of different professional bodies has been made. An audit approach which has been well recognised has been described. The audit procedures followed as described by the organisations which have been included in the sample has been analysed. Similarly five leading firms of statutory auditors have been approached and the procedures that they follow while auditing on a computerised environment had been noted by way of answers obtained from them on the questionnaire provided to them. The hypothesis for this thesis is that the controls and auditing standards in a computerised environment as prevailing in India is inadequate. The analysis of the control
procedures in organisations and the audit procedures followed as reported by the organisations and the audit approach as mentioned by leading auditors have been undertaken to verify the hypothesis.

The information technology security problems become very vital and important as most organisations have automated their activities. Even electronic links are being established with their trade partners (EDI EFD). Taking advantage of the technological developments organisations are computerising extensively. Along with this development the security problems are also on the increase. Most of the companies have some inadequacy or the other in their IT security. Organisations are failing to wake upto this problem while as now in our country there have been no formally reported cases of fraud and losses.

Taking into consideration the experience of other countries, it would be a matter of time before sophisticated crimes and frauds associated with computers would be as common place as frauds in a non-computerised environment.

Macro Kapp, Director, Coopers & Lybrand, London in his presentation "IT Security in a changing world" at the South East Asia Regional Computer Conference, December 1989 discussed the possible problems and estimated that worldwide losses caused by IT security would be $15-30 billion or so. A body of French Insurance Industry, APSAIRD has published data for France in the year 1987. The table below gives the detail. It is very shocking and revealing to note that more than 72% of the losses are caused by

(a) System Design Programming Errors

(b) Fraud Software Sabotage
(c) Theft and disclosure of data
(d) Theft of software.

Data regarding losses due to IT security are available for countries other than India. In advanced countries, Auditing Techniques are trying to keep pace with technological development. In our country technological development have been taken advantage of and specially during the last decade. The impact of computerisation on organisations has been very very significant. However, the aspects of control and audit has been lost sight of under the impression, most probably that companies are falliable and hence personnel and systems associated with the computers have to be infallible!!

It is in this context that the aspect of making a study of the control procedures that need to be implemented in different computer environments and the corresponding audit methodologies to be adopted has been undertaken to evaluate the adequacy of controls and take preventive, detective and corrective steps to minimise the impact of possible losses.

SCENARIO IN OTHER PARTS OF THE WORLD

A new pattern of computer related crime is emerging. It is characterised by a shift from insiders to outsiders and from applications to systems. The risk is to management in general, but computer auditors in particular. In response to this pattern, computer auditors may wish to leave the audit of applications to others and shift their focus to systems. In the earlier decades, it was speculated that there would be exploitation of system vulnerabilities. But what was actually seen was the
exploitation of application vulnerabilities. There was a concern about interference with or contamination of the application programmes by unauthorised people. What was seen was manipulation of the input by authorised people! The computer auditors emphasised shift to applications.¹

There was speculation about attacks from outsiders. What was actually happening was that there were attacks by insiders. It became clear that while system access controls were necessary, they were not sufficient. People could not be relied upon to behave safely. In such circumstances, access controls would not be effective.

The emphasis of the auditor shifted to such areas as password management, separation of duties and user accountability. It is reported that the traditionally managed systems are contributing to the vulnerability. The analysis of the attacks which had been studied demonstrate that serious problems would be caused and they are likely to be in the increase.¹

The contributing factors:

(i) There are large number of privlege users on the target systems. In some cases, all of the users are privileged. In many cases, privilege on one system transmits into priviliging on nearby system. The analysis proved that if a hacker is able to gain privlege on a system, he is able to change passwords on dormant accounts and add "secret doors" he can contaminate the system.


in such a way that it will be impossible to exclude him without seriously disrupting operations.

(ii) The second factor is the continued reliance on re-usable passwords. This leads to vulnerability to dictionary attacks.

(iii) The presence on the system of active but rarely used passwords.

(iv) The presence on the system of widely authorised and used, very general, fully privileged but otherwise insecure programmes. The statistics prove that the sample of 150 MVS systems 103 (67%) had one or two more of these programmes and of these 88 (85%) still had the default lockwards in place. An analysis of various instances of attacks on the computer suggests a shift in the source and nature of the exposure. These exposures are so widely documented that any exploitation will be extraordinarily embarrassing to management and to computer audit. The study recommends that while auditors are not responsible for preventing computer related crime, they are responsible for identifying and reporting to management conditions which contribute to the crime.

The recommendations of the study have been as follows:

(i) Identify and report excessive privilege

The auditor should identify all user profiles that contain system management privileges. The presence of more than one should be reported.

Identify and report programmes that run with system privileges. Application code and system management code should run in application state with the privilege of the user. The auditor should identify and report all such codes that run with the system privileges. The auditor should look for and report any evidence that these
programmes were available to others. The use of the default lockwords to one such evidence.

Identify and revoke dormant profiles

A large number of such profiles constitute a risk to the system and should be remedied.

Identify unused or unnecessary ports

The auditor can contribute appropriate management consideration. Any evidence of unused or unnecessary codes were reconciling the presence of system codes to their use and also by examining the process by which such decisions are made.

The recommendation reflect standards of practice that the auditor should expect. These practices are motivated by emerging exposure to outsider attack. However, these can be expected to reduce the exposure even more from the likely threats from insiders.

Statistics have been provided on the computer crime. The statistics has been collected from 3 discreet surveys. The 1986 computer crime survey consisted of contacting 250 prosecutors’ offices. 75 cases were reported.¹

¹ Computer crime and abuse by J.J.Buck Blook Becker EDPAA Audit Journal, Volume II, 1990,
In 1989 computer survey consisted of mailing to 2500 prosecutors' offices in US.

The third survey conducted in late 1988 was with the cooperation of the information systems security association. The survey went to 3500 computer security professionals. Approximately 14% responded.

**Computer crime availability of information**

On the basis of the three surveys, it was clear that very few computer crimes are reported to prosecution authorities. The chart (1.1) on responses to serious security incidents shows that as against 2% in 1987 it was 6% in 1988. The research further proved that any study of reported computer crime cases may not be representative of the universe of "serious security incidents" known to the respondents in the centre survey. There was a survey conducted when computer security professionals were asked for "known information security losses" for 1988. The average loss reported was $1,09,000. Figure 1.2 represents average annual computer abuse loss.

In 1986 theft of money represented almost half of all prosecuted computer crime cases and theft of services represented only 10%. By 1988 money theft exceeded theft of services only 36% to 34% (Figure 1.3).

More than half of the cases in our natural sample of computer crime prosecutions involved losses of $10,000 or less only 125% involved losses of $1,00,000 or more (Figure 1.5).
The National Centre for Computer Crime Data (NCCCD) published an analysis for which focused on the California (USA) data (Fig.1.6). Computer Professionals predicted phenomenal growth in software products to prevent virus attacks (Fig.1.7).

Trends in Computer abuse

The National Centre for Computer Crime Data has the opportunity to compare the make up prosecuted cases before 1986 and after 1986. They have attempted to infer some significance from the changes and they are as follows:

No significant development is the growing evidence of the vulnerability of computer communication networks.

Figure 1.4 details the types of the computer crimes. Computer security professionals predicts enormous growth in the use of software to prevent viruses. However, it was proved that viruses are less of a concern than down time, destruction of data or extraordinary disclosure of data.

Implications of computer crime

Computer crime become a media issue whenever a major case comes up. Wise computer security professionals and auditors have been able to convert public interest in crime to enlarged budgets for computer security efforts. The survey finally concluded that controlling computer systems to reduce computer crime is a serious challenge. The problem has been growing and the assets which can be broad to bear against computer crime have also grown. The authors have concluded that the key
**FIG 1.1: RESPONSE TO SERIOUS SECURITY INCIDENTS**

![Bar graph showing the number of total incidents and resulting prosecutions for 1987 and 1988.](image)

<table>
<thead>
<tr>
<th>Year</th>
<th>Total Incidents</th>
<th>Resulting Prosecutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1987</td>
<td>335</td>
<td>8</td>
</tr>
<tr>
<td>1988</td>
<td>485</td>
<td>31</td>
</tr>
</tbody>
</table>

(Represents 2% in 1987 and 6% in 1988)

Source: NCCCD and RGC associates
FIG 1.2: AVERAGE ANNUAL COMPUTER ABUSE LOSSES

Source: NCCCD and RGC associates
FIG 1.3: TYPES OF COMPUTER CRIME


Money Theft

Software Malicious Deceptive Theft of Services

Harrassment Extortion

Malf. 1986 1988
FIG 1.4 : RELATIVE SERIOUSNESS OF THREATS

Source: NCCCD and RGC associates
FIG. 1.5: COMPUTER CRIME LOSSES
(All Figures in %)

Sources: NCCCD, Computer Crime Census '88
FIG. 1.6: RESULTS OF CALIFORNIA ARRESTS
(All Figures in %)

Convicted 71

Dismissed by court 14

Dismissed by D.A. 15

Source: NCCCD, Computer Crime Census '88
FIG 1.7: USE OF TECHNOLOGY/PRODUCTS IN 1985, 1988 & 1991 (CHART 1)

% Percentage of Users

Mainframes/Mini | Smart Cards | Call-Back Modems | C2 Products | Division B Products | Division A Products | DES Encryption


Sources: NCCCD and RGC Associates Security Survey
FIG 1.7: USE OF TECHNOLOGY/PRODUCTS IN 1985, 1988 & 1991 (CHART 2)

% Percentage of Users

Sources: NCCCD and RGC Associates Security Survey
to this problem is commitment. There is need for generating commitments to security. Technological solutions would not solve the problem.

Computer abuse in Australia

Statistics recently released by Australian computer Abuse Research Bureau identify that reported computer abuse incidents have increased dramatically. Nine years the Bureau collected reports of 205 cases representing almost $11 million. In 1989 alone, there were 51 reported cases representing $2.6 million. In the 10 years that the bureau has been in operation they have identified a number of interesting aspects relating to the TOP 9 TEST was a measuring mechanism developed by Gerry Bonbow and his friends. C appendix top tests. Of the 392 responding organisations .02% pass the test with 60% of the respondents not receiving a ranking at all. The study was reperformed recently with the same poor results.

Industrial groupings

ACARP statistics confirm that approximately 36% of computer fraud by value is performed in the financial sector.

Fraud reporting

There is an understandable reluctance to publicly disclose information which is considered confidential and computer abuse falls into that category. In Australia it is observed that a computer crime is performed in 80% of instances by internal

---

employees and yet only 20% of the organisations are prepared to perform security evaluations on prospective employees. It is reported that in 1984 the American Banking System electronically transmitted in excess of $180 billion everyday. It is reported that "given the known statement of computer security this is not a surprise that computer experts around the world are on the edge waiting for an organised attack which should spell disaster for corporate identities either to consider invincible".

OBJECTIVES OF THE STUDY

The basic hypothesis for this thesis is to prove or disprove that controls in a computer environment as they exist now are insufficient and that auditing practices followed to evaluate the controls and report on them are well below the accepted standards.

In specific terms, the objectives of this study are to:

(1) Identify existing control systems select types of computerised environments (Personal Computers, End User Computing, LAN, DBMS etc.) ;

(2) Review the procedures which the selective auditors are adopting in those computerised environments to satisfy themselves that the internal controls are adequate in terms of the completeness, accuracy and reliability of the information which forms the basis of the financial statement of the organisation;

(3) Examine the levels of efficiency of control procedures in the light of well-laid out standards of controls in different environments;
(4) Evaluate overall level of controls meant to ensure the appropriateness of audit requirements; and

(5) Suggest suitable control mechanism to improve effectiveness of audit practices in a computerised environment.

SOURCES OF DATA

Study is based both on primary and secondary data. The secondary data sources are well-known publications of studies effected in USA, and UK. Primary data is that personally collected from organisations and auditors.

Secondary data

1. Systems Auditability & Control Reports published by Institute of Internal Auditors USA.

METHODOLOGY

To generate plausible hypothesis for study a focus group discussion was adopted with experts fully conversant with EdP auditing practices and then the consensus from the group was stated as an initial hypothesis for further research in this study.

The actual methodology adopted for this research falls under the category of indepth case study method. There are two typical methods available for doing
research with empirical data. One is large sample survey method and another indepth case study method. Generally large sample survey method is resorted to when the system being studied or being researched is very familiar to the respondents and they can correctly interpret and answer the questions posed to them. Wherever for the first time a research is undertaken to study the performance of any system, it is preferable to have a detailed checklist of relevant questions pertaining to the study which could be personally administered by the researcher so that he/she can clarify the meaning and interpretation of the questions to the various respondents. In that process, additional insights can be obtained about the performance of the system thorough personal discussions. Understandably, the number of such cases cannot be too large to facilitate indepth discussion. So in this research, the study has the second method of indepth case study. Also in this method the number of organisations and the number of respondents taken are not too large. Hence conventional statistical tests for validating the responses will not be meaningful.

Selective data which is not biased has been selected for sampling purposes. Leading audit firms who have extensive clientele both in public sector and private sector, operating in different areas of financial, marketing, manufacturing etc. had been chosen. As regards organisations, which have been using computers a sample size of 30 was tested. As leading auditors were contacted for auditing methodology adopted by them, data would represent audit procedures adopted in more than 100 organisations.

As regards computerised environment, the sample size of 30 installations include different types of management like public sector, private sector, public limited companies, private limited companies, financial institutions, banking etc.
The methodology and sample size are defended on the following grounds:

1. The findings of the study are though substantially based on the responses to the questionnaire still considerable personal intervention has taken place with the Managers concerned to get deeper insights into their problems and state of affairs. This would not be possible if a larger sample is taken.

2. (a) The organisations chosen for the study are typical of most of the Indian Commercial organisations.
   (b) The auditors interviewed are also the reputed ones.
   (c) The variation in the responses in the sample organisations/auditors is practically nil. This gives substantive credibility to the findings and hence generalisations also are valid.

The fundamental principle in sampling theory that lesser the variation in responses small sample will be adequate has been adopted.

LIMITATIONS OF THE STUDY

The study has the following limitations:

a) The data for the study is not voluminous though illustrative. This is due to the fact that a representative sample which has not been subjective has been chosen.

b) Throughout the study no distinction has been made between different management styles of the various organisations. This is due to the fact that though the style of management may vary the concept of basic accountability of top management does not cease.
The auditors selected are mostly seniors and well established in the profession. Juniors and freshers have not been many in the sample. This is due to the fact that larger organisation with wider computerisation are mostly audited by seniors. However, in the smaller organisations, it is mostly PC based and controls in PC environments have been fairly well covered in the samples.

ARRANGEMENT OF THE CHAPTERS

The thesis has been divided into nine chapters. Chapter II deals with auditing standards where the need for standards is emphasised. The professional pronouncements in the form of Standards of international bodies like the American Institute of Certified Public Accountants. Institute of Chartered Accountants of England and Wales, Institute of Internal Auditors, USA, EDP Auditors Association, USA are referred to with special reference to those standards which are applicable to auditing in a computerised environment. Reference is also made to ISO-9000-3, wherein quality standards required for software development are specifically mentioned.

Chapters III, IV, V and VI deal with controls in specific environments. Four important and more commonly used environments have been chosen. Chapter III deals with controls in End-User computing. The reasons for the rapid growth of End-User computing, control concerns and audit considerations are also highlighted. A copy of the questionnaire which was used to make a sample survey of five organisations having End-User computing is enclosed. The findings at the end of the chapter are based not only on the information collected from the responses to the
questionnaire, but also of the research team of the US of Institute of Internal Auditor as published in their Report, "Systems Auditability and Control".

Chapter IV deals with Local Area Network. A technology overview is provided. The current utilisation of LAN in different organisations are discussed. Accepted procedures regarding the establishment of controls and auditing procedures are discussed. A sample questionnaire to evaluate the controls in organisations having LAN is enclosed. This questionnaire was utilised to secure responses from five organisations and a comparison of existing practices for implementation of controls and audit procedures in these environment is compared with accepted controls and audit procedures in a local area environment. This is followed by analysis and findings. The findings include my own based on the responses from five organisations as also the IAA's findings as reported in SAC. The suggestions regarding effective implementation of controls in a LAN and specific audit procedures needed form the subject matter of the section regarding suggestions.

Chapter V deals with the topic of Database Management System (DBMS). While explaining the concept the specific vulnerabilities of the environment and the steps to be taken to plug the loopholes are discussed. The procedures and systems as followed in organisations which have implemented the DBMS is discussed. The standard accepted procedures, control objectives and audit guidelines in a database management system environment are stated. The controls and audit procedures as they exist are compared with norms. The results are analysed and the findings reported. The findings also include those reported in SAC of IAA. The final section contains suggestions regarding implementation of controls and practices of the acceptable audit procedures.
Chapter VI deals with controls in a UNIX environment. The operating systems UNIX had been the subject matter of controversy. It was even stated that "UNIX security" is a contradiction in terms as the original version of the operating system UNIX had a great deal of vulnerabilities. Over a period of time, later versions had attempted to plug the loopholes. Many proprietary operating systems of UNIX have also been supplied by vendors. A general discussion on UNIX operating system with possible loopholes and attempts made by subsequent versions of different vendors to plug the same are also discussed. Special audit concerns in this operating system and how the auditor should audit the system by UNIX itself are discussed. Based on the questionnaire enclosed, responses have been obtained from five organisations and analysis and findings have been reported. Suggestions for implementation of effective controls and proper procedures to be adopted by auditors are discussed.

Chapter VII deals with Disaster Recovery Plan. The importance of Disaster Recovery Plan is highlighted and instances of successful disaster recovery plan (DRP) and failures due to the absence of DRP are highlighted.

The anticipation of possible exposures and providing for the same is discussed. The contents of DRP, the method of implementation and review are highlighted. The role of the auditor with regard to the disaster recovery plan is discussed.

A sample questionnaire for collecting information from a sample of 30 organisations is enclosed. Analysis of the findings have been reported. Suggestions for effective implementation of DRP and the role of the auditor are also brought out.
The technological developments are continuously taking place in the area of development, storage, communication, database etc. Concepts of CASE tools, Re-engineering and EDI have been highlighted. Control objectives and audit concerns in these areas have been discussed and, included in the chapter "Summary, Conclusions and Recommendations".

Chapter VIII deals with an audit approach. Without considering any specific environment, a general approach which an auditor should have when auditing a computerised environment is highlighted.

The current scenario is discussed briefly. A detailed discussion on well-accepted approaches for auditing in a computerised environment is attempted giving the various steps and the tasks involved in each step. A sample questionnaire is enclosed to illustrate information regarding the approach of auditors as currently practised.

Practising Auditors' responses for the questionnaire has been analysed. This is also supported by information gathered from a sample of 30 organisations regarding audit practices of their respective organisations.

Chapter IX presents a summary of the findings and draws an overall conclusion.