CHAPTER IX

SUMMARY, CONCLUSION AND RECOMMENDATIONS

This Chapter presents a summary of conclusion and recommendations of the study besides making useful recommendations in control standards and auditing procedures in a computerised environment.

AUDITING STANDARDS

International bodies like the American Institute of Certified Public Accountants, Institute of Internal Auditors, USA, the Institute of Chartered Accountants of England and Wales, United Kingdom, EDPAA Foundation, USA, have issued official pronouncements regarding the auditing standards to be observed in a computerised environment. Though there may be no enforcing authority insisting on the auditors observing certain procedures it is quite necessary for the auditors to change their approach and adopt appropriate tools and techniques while auditing in a computerised environment.

The innumerable instances of frauds which have occurred in a computerised environment reported elsewhere in the world (as mentioned in Chapter I) proves beyond doubt that it is absolutely imperative for the auditor to acquire adequate skills and competence. In the absence of such skill and competence to certify that adequate controls commensurate with size and nature of the organisation exist is meaningless. In addition, in the absence of adequate knowledge of necessary internal
controls in different computerised environment, the auditor will not be able to satisfy himself that they represent a true and fair view.

CONTROLS IN END-USER COMPUTING

The practice of end-user computing has been proliferating due to the fact that the cost of hardware and software has been falling significantly and they have been becoming very user-friendly. In addition, more and more users have become more computer-literate and hence usage of computers, specially PCs by functional departments, has become very common. However, the study reveals that there are no policies and procedures regarding the control and security in a computerised environment. Well-accepted control procedures are absent. Neither the management nor the user is in full realisation of the consequences of installing end-user computing without implementing the necessary discipline which comes with it. Neither the internal auditors nor the external auditors are seized with the responsibility of the accepted procedures if audit review have not been followed.

CONTROLS IN LAN

With the development of information technology and communication and with the availability of communication software, many organisations have taken advantage of this concept. Needless to say there are additional control features which need to be adhered to in a net-worked environment using advance communication facilities. The net-working environment is a few further steps in technological development. The auditors have not acquired adequate skills and competence in our country even for auditing in a basic computerised environment. In view of this, they are not even
aware of the necessary controls in a net-worked environment. Hence the adequacy of auditing practices does not arise. The auditing standards as practised now are totally inadequate.

**CONTROLS IN DATABASE MANAGEMENT SYSTEM**

Database management system is an extremely useful technology and many vendor packages like ORACLE, INGRESS and SYBASE are in the market vieing with each other; after realising the utility of DBMS certain large organisations have implemented the same. However, a study of a sample number of organisations reveals that the control procedures and practices are in line with the accepted norms in toto. As regards the audit procedures apart from the organisations reporting that neither the internal auditor nor the external auditor have ever reviewed their controls, the auditors themselves have conceded that they are not even aware of the control objectives and audit concerns, thus proving again that control practices and auditing standards in a computerised environment.

**UNIX ENVIRONMENT**

This particular operating system can be chosen as when it was introduced it had a number of loopholes. The organisations who introduced the system realised it after introduction and even by a process of control trial and error, are trying to plug the loopholes. A study of the practices in the organisations which have implemented UNIX reveals that all of them have had an unpleasant experience or two when the vulnerabilities in the operating systems have been exploited by a process of evaluation, securities are being built into this environment. However, in most of the
organisations the system is not fool-proof. As regards the auditors they are totally unaware of the concept of operating system vulnerabilities in general and UNIX operating system in particular.

**DISASTER RECOVERY PLAN (DRP)**

It is extremely important that once the systems have been computerised there should be a disaster recovery plan. There are well-established procedures and guidelines for evolving a plan, implementing it, maintaining it and constantly reviewing it; It is an on-going process. However, in practice the organisations, mostly, do not go beyond maintaining a copy of the programme and data, that too in the same building in the same computer department, mostly in the cabin of the Systems Manager. The organisation, specially the computer department is aware of the risks involved. However, the study reveals that neither the management nor the data personnel departments have seriously done any thinking of evolving an effective disaster recovery plan. Auditors do not realise that information is an asset. While evaluating and verifying the existence of assets information is left out of count. The fact that there is no insurance coverage other than for the hardware is totally lost sight of. In the absence of any knowledge of the contents of disaster recovery plan and also the absence of any awareness for the necessity of disaster recovery plan, auditing involvement in evaluating the existence of disaster recovery plan and its adequacy is totally absent.

**SUMMARY AND CONCLUSIONS**

An analysis of the appropriate controls in specific computerised environment reveals that it is far below acceptable norms. The concerned auditors, both internal and external are totally ignorant. The analysis of the financial statement and findings
substantiate the NULL hypothesis that control standards are inadequate and auditing invisible and hence inefficient.

Questionnaires for Physical security (Appendix A), for Personal Security (Appendix B), Data security (Appendix C), Application software security (Appendix D), Systems software security (Appendix E), Telecommunication security (Appendix F), Computer operation security (Appendix G) were used to collect data and quantify the risk assessment under each of the areas. The results as obtained are given in table 10.1.¹

The table as given below contains risk ranking worksheet was utilised.

Table - Risk-Ranking Worksheet

<table>
<thead>
<tr>
<th>Computer Security Area</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>Physical Security</td>
<td>0-26</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>0-34</td>
</tr>
<tr>
<td>Data Security</td>
<td>0-44</td>
</tr>
<tr>
<td>Applications Software Security</td>
<td>0-64</td>
</tr>
<tr>
<td>Systems Software Security</td>
<td>0-42</td>
</tr>
<tr>
<td>Telecommunications Security</td>
<td>0-39</td>
</tr>
<tr>
<td>Computer Operation Security</td>
<td>0-33</td>
</tr>
</tbody>
</table>

The data obtained was analysed utilising the norms provided the above table. The analysis of the sample survey if 30 organisations was as given in the following table:

It will be observed that out of the 30 organisations, 29 organisations were in the high risk category in areas of systems software security, telecommunication software security and computer operation security. 28 of the 30 organisations were in the high risk category and two in the medium risk category in the areas of Personnel security, data security and application software security. There was only one organisation in the low risk category and 2 organisations in the medium risk category and the balance of the 27 in the high risk category under the category of Physical security. It is of significance to note that out of the 30 organisations one organisation which had low risk in 2 areas and medium risk in 6 areas was a multi national company which had auditors coming from abroad. The head office of the organisation in U.S. which had offices all over the world had laid down standard procedures and guidelines for security aspects and audit procedures.
### ANALYSIS FOR RISK ASSESSMENT (Table 10.1)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>28</td>
<td>58</td>
<td>49</td>
<td>68</td>
<td>42</td>
<td>43</td>
<td>43</td>
</tr>
<tr>
<td>2</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>3</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>90</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>4</td>
<td>60</td>
<td>93</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>5</td>
<td>50</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>6</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>7</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>8</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>9</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>10</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>11</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>12</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>13</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>14</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>15</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>182</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>16</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>17</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>18</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>19</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>20</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>21</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>22</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>23</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>24</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>25</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>26</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>27</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>28</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>29</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
<tr>
<td>30</td>
<td>60</td>
<td>103</td>
<td>96</td>
<td>172</td>
<td>100</td>
<td>86</td>
<td>86</td>
</tr>
</tbody>
</table>
AUDIT APPROACH
AND
RECOMMENDATION
AUDIT APPROACH

A study of the general approach in a computerised environment reveal that auditors of large organisations which have complex computer environment have not followed any of the accepted procedures. As a matter of fact, the controls of the general questionnaire seemed incomprehensible responses to them. Questionnaire in Appendix I was negative in all the cases. The general view expressed was that senior executive in charge of computer operations in their client's offices were very competent and reliable. Again apart from the supporting evidence collected from well known auditors it was supported by their clients also. They had no hesitation in stating that the controls in a computerised environment have never been evaluated either by the internal auditors or the external auditors. A study of the controls and the auditing standards supports the NULL hypothesis, controls are insufficient and auditing standards are woefully inadequate.

RECOMMENDATIONS

It is more than overdue that the management and the auditors should realise the impact of computerisation on auditing. While the objectives of auditing have not changed the means of achieving those goals and objectives have definitely changed. Hence, it is necessary for the management to ensure that controls in the computerised environment introduced in their organisation are adequate. They should also be seized with the necessity for a disaster recovery plan. With these objectives, they should equip their internal audit department with staff competent to evaluate the adequacy of controls. In case it is not possible for them to immediately train the personnel of the internal audit department to acquire adequate skills and
competence they should include in the audit team an information technologist, who is competent and knowledgeable of the specific computerised environment in their organisation. In the absence of such a staff, the possibility of frauds associated with computerised environment cannot be ruled out. It is better to take preventive steps. As the computers are sophisticated, knowledgeable computer personnel with fraudulent intentions may hold the organisation to ransom. Apart from financial loss the organisation would also suffer loss of image.

The statutory auditors cannot hope to protect themselves for improper discharge of their duties as auditors in a computerised environment. Absence of auditing standards which make it obligatory to observe certain procedures may not preclude their being sued for negligence. The auditors should equip themselves to meet the challenges of fast-changing technology. It is recommended that large auditing firms should have an EDP Cell. The personnel should consist of people knowledgeable about general and application controls in a computerised environment, as also of controls specific to certain computerised environments. Their skills with the experience of auditors would help to discharge the responsibility to the management, the shareholders and the public. They should also consider seeking the services of specialists in the field and relying on the specialists' opinion regarding adequacy of controls.

The technology is developing very fast. In the existing computer environment itself controls are not satisfactory and auditing methods inappropriate. In the following pages, a brief review of the Emerging Technologies is provided to highlight
the widening gap between development of technology and controls and auditing standards.

EMERGING TECHNOLOGIES

To remain competitive and be able to respond quickly to global markets organisation need to change and they are changing. The concept of tele-commuting from anywhere in the world to any other place in the world and to his office in the home town has become a reality and a necessity. It is possible to have a personal computer net-worked into the office systems. This in turn would have access to electronic mail and support of fax facility. This gives enormous power to the user; he is able to obtain information from the system. Along with the advantage there is a disadvantage in that it provides the user with the capacity to destroy or modify any information. This leads to a situation when data security becomes a major issue. The Institute of Internal Auditors Research Foundation of United States of America in its research project "Systems Auditability and Control Report" as reported in Appendix A of Module II, has analysed the most frequently reported risk for information technology components. One of the components that has been considered is emerging technologies; the given survey findings and observations relating to emerging technologies are as follows:

Most frequently reported risks for Information Technology Components:

* Forty six per cent of the 254 respondents indicated that one of the highest risks is unauthorised access or changes to data or systems. Of this 46% (117 respondents), 30% felt the risk would decrease in the
future, 25% felt there would be no change, and 45% said it would increase”.

Emerging technologies has been classified under the following heads:

i. Development
ii. Storage
iii. Personnel
iv. Communications
v. Data base
vi. Interface
vii. Knowledge based systems

Development methodology

Examination has been made of the emerging technologies that support applications system development; i.e. the technology which facilitates development of systems and the corresponding programmes. The two main points which have been considered are:

i. CASE (Computer Aided Software Engineering) and
ii. OOP (Object Oriented Programming)

i. CASE

It is a software technology which has been developed to increase productivity and improve software quality. This has been achieved by introduction of product standards and analysis. The usage of CASE technology is also expected to decrease the cause of documentation and maintenance of application systems.
Generally the CASE products are classified under two heads:

i. **Upper case**: This deals with a strategic planning to requirements definition, proto-typing and systems module design

ii. **Lower case**: This deals with code designing and code generation, testing for maintenance.

It is reported that the most widely used case tools are analysis, work benches, auditors, debuggers, compilers and test tools. It is reported further that the code generators are very specified and may even produce up to 85% of the code for a given application. It is reported that great saving will be realised in maintenance. Automatic production of documentation is a much appreciated incentive where large products of system development are involved. It is reported that this has been greatly appreciated by the US department of Defence Programmers. Using of CASE technology has been found to be useful in re-engineering. Re-engineering is a process by which the existing software systems are modernised so that their functional lives could be prolonged as also preserved. The value of the existing system of re-engineering consists of three components, viz.

i. Reverse engineering

ii. Forward engineering

iii. Code generation

In the first phase, viz. reverse engineering, the system as it exists is analysed in detail and categorised into its component definitions. In the forward engineering, the existing system is functionally enhanced to a new technology platform. In the final phase, viz. code generation the programmer generates the needed codes from the component definitions.
While in America, it is reported that CASE tools are extensively used. It must be observed that even in our own country, leading software consultants are making extensive use of these tools while offering their services to the various organisations for software development. The tool has certain risks, controls and audit considerations associated with its usage. They are as follows:

i. Auditability
ii. Accuracy
iii. Integrity

The CASE environment and maintenance

Certain tools for data integrity by including validation and authorised access. If these tools are not properly managed, it would result in loss of data integrity.

CASE tools need to be consistently used. If it is inconsistently used to define business tools, it would lead to development of improper systems which in turn would lead to significant business risk.

SECURITY

It is very important to protect proprietary data from unauthorised access. If such a protection is not there, it would lead to proprietary and strategic data being disclosed to unauthorised people which may result in a business risk.
STANDARDS

There are no common standards for all CASE tools. This may lead to a situation when different CASE tools with differing standards being used in the same environment. This may cause incompatibility and duplication of efforts.

ADMINISTRATION

Proper use of CASE information is absolutely necessary. To achieve this, there has to be effective administration and control of user access. When CASE tools are used for Reverse Engineering the main objective is to create new and important versions of software. In the absence of adequate administrative procedures there is a possibility of risk that multiple versions of the same software may be created which may result in confusion.

Costs associated with implementation of CASE should be justified from the angle of the benefits arising therefrom.

CONTROLS

CASE tools themselves have facilities and features for control purposes. These could be effectively utilised for implementing in a CASE environment. Some of the controls are as follows:

To obtain accurate and complete documentation the repository can be utilised as an effective control tool. CASE tools have their own access control features. These
can be utilised to enforce only authorised access to the information in a CASE environment.

The risk of inadvertent data corruption and improving productivity can be achieved by using the functions of CASE tools which have their own rules for maintaining data integrity, validation and access.

Risks associated with data accuracy and integrity could be mitigated by having end-user involvement while the systems are being developed.

Use of change management procedures in the systems development process is another important control in the CASE environment. Many CASE tools have version control features as well as authorisation and sign off functions.

CASE tools for auditors

An auditor could perform specific audit tasks by utilising CASE features and functions. Given below are some of the examples of situations in which the auditor could use CASE tools.

i. System can be understood and the controls could be documented by making use of the repository as an information source. When the question of "wire use" arises the repository could be used as an audit trail. It is necessary for the auditor to become familiar with CASE tools as these tools represent possible increased risks. However, by understanding and mastering these tools the auditor could use them as control and auditing tools.
OBJECT ORIENTED SOFTWARE

In the conventional programming the object of problem solving was procedural while in object oriented programming it is not so. Mr. Grady Booch, an ADA expert sums up the difference between object oriented programming and procedural programming as follows: "Write the specifications of the software you want to build, underline the verbs if you are after procedural code; nouns if you aim for an object oriented program.

RISKS AND CONTROLS

Object oriented software is a totally new technology; there are certain inherent risks; some of the risks are: There is concern regarding accuracy and integrity of the contents of the objectives as the implementation of OOPS stress that the content of an object can be "hidden" from the program.

If careful management procedures are not applied, there is a risk that the accuracy and integrity of the libraries associated with the OOPs may become questionable. It is likely that the implementation of OOP there may be a degradation of performance.

However, these new technologies provide possibility for applying innovative approaches and implement new and more reliable controls.

The techniques for implementing controls in OOP environment are totally different from those in traditional programming objects. The auditor must have adequate knowledge to understand and evaluate controls in this new technology.
STORAGE TECHNOLOGY

Magnetic storage have been the traditional medium of storage. Recent developments have proved that optical storage is technically better and provide many more attractive benefits like greater storage capacity, longer storage life and better error detection and correction mechanism. However, there are certain reasons associated with this technology like increased exposure to data loss or theft. This is due to the smaller size of the medium.

PROCESS TECHNOLOGY

Even in the area of processing technology there have been emerging trends and the two main technologies are (i) Co-operative processing and fault tolerant computers.

i. Co-operative processing

In co-operative processing machines have separate portions of application. However, they work together to accomplish common processing objective.

Data that resides on computers in different locations is accessed. In a co-operative processing environment the processing power and data are distributed across a computer network.
Risks, controls and audit considerations

Co-operative processing technology works in a multi-processor or multiple machine environment which leads to the boundaries of the applications being less discreet than those of traditional processing applications.

RISKS

Audit accuracy and integrity: Because many and different hardware and software environments are involved, there is a possibility of risk of incompatible versions and unsatisfactory change management procedures.

In view of different locations being used there is a replication of data and files. If there is a possibility of risk of these files not being properly synchronised with the master copy.

SECURITY

In a co-operative processing data is moved from the main frame to microcomputers. These microcomputers may not have adequate CASE controls to protect data from unauthorised use.

RECOVERY AND BACK UP

Recovery and back up procedures require more detailed planning.
ERROR HANDLING AND ADMINISTRATION

Error handling process would be compromised if there are not sufficient controls. However, there are controls which could minimise, if not eliminate these risks. Some of them are as follows:

When an information system spans multiple computing environments special care should be taken to ensure adequate co-ordination of activity. The designers and implementors should take adequate steps to minimise the risk of un-co-ordinated processing to mitigate the risk of absence of synchronisation. Special software could be designed. It should automatically modify all tables and files at periodical intervals.

Change management procedures should be controlled strictly.

As restart and recovery procedures are complicated the designers and developers and users should ensure that the co-operative processing software has features and functions which will facilitate recoverability.

AUDITORS

Auditor should be aware of the inherent risks and assure himself that there are adequate controls which would minimise the risks.

Co-operative processing will require new audit trail and system recoverability controls.