CHAPTER III

END-USER COMPUTING (EUC)

Overview

The technological developments in the computer field have made computers "User friendly". Users tend to use local computing power which has resulted in tremendous growth of End-User Computing. The user instead of depending upon a central computer department and its staff to render assistance in using computers for its department depends upon itself. End-User Computing as "user created or acquired systems that are maintained and operated outside of traditional information systems (IS) controls."
Figure 3.1

END-USER COMPUTING RISK CONTROL LEVELS¹

High Controls Required

Moderate Controls Required

Minimal Controls Required

There are many reasons for this rapid growth of this trend:

(i) There is always backlog of projects and the priorities which the user may have for its application may not be the same for the centralised computer department.

(ii) The user's desire to have direct control over their applications.

There are different types of end user computing activities:

Single user

(i) Stand-alone PC: This may be used by a single department for routine preparation of some reports.

Multi-user

(ii) It may be used for preparing adhoc reports using software like spreadsheet etc.

(iii) Business applications may be developed which are of immediate use to the department.

Different users may be utilising the services of the same PC.

The PC may be one of the nodes in a LAN environment when the node may be used for not only developing routine reports but also to access commonly available data on the network.

Special reports useful for achieving the goals and objectives of the department.
AUDIT RISKS AND CONTROLS TO BE EVALUATED

<table>
<thead>
<tr>
<th>Bar 1</th>
<th>EUC Risks and controls</th>
<th>Traditional IS Risks and Controls</th>
</tr>
</thead>
</table>

**Level of Technical Support Required by Users**

<table>
<thead>
<tr>
<th>Bar 2</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>N/A</th>
</tr>
</thead>
</table>

**Level of Control Required Over System**

<table>
<thead>
<tr>
<th>Bar 3</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
</table>

**Level of Technical Auditing Expertise required**

<table>
<thead>
<tr>
<th>Bar 4</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very High</th>
</tr>
</thead>
</table>

The specific advantages of end user computing are that

(i) It helps in satisfying the increased need for analysed data and respond to queries.

(ii) It meets one time requirements by developing temporary systems

(iii) It reduces the normal user and computer department conflicts by providing users with more direct operational control over the system.

The development cycle is shortened, as the realisation of priorities by the user is more than the DP department.

It is in keeping with the general corporate policy to decentralise activities.

As against the advantages, there are certain disadvantages. The following are likely to occur:-

---

(i) As there is no centralised effort in pooling resources experience and skills, the end-user may not have appropriate appreciation of the associated risks. Users in their over enthusiasm tend to tackle tasks which are beyond their capability. With the desire to keep up with the latest technology, hardware and software may be acquired which does not justify the business needs.

Delegation of decisions not in keeping with position of responsibility of individuals may take place.

There are many control issues in the nature of

(a) inconsistent data
(b) Incomplete information trails
(c) Poor system change controls
(d) Poor documentation
(e) Poor security
(f) Inadequate back up and recovery procedures
(g) Software security.

PROBLEM AREAS

In view of the declining costs and increasing importance of information on timely basis, the awareness and the need for end-users themselves to have the computer facility has been on the increase. Users have become self-reliant and feel that they do not have to bear all the over-heads that are allocated to the department
for the services rendered by the centralised computer department. The end-users make extensive use of spread-sheets and word processing facilities.

The more enterprising of the staff in user departments have acquired working knowledge of using the computer and the software. It cannot be claimed that the knowledge of such users is of a high level. The situation as it exists in many organisations is as follows:

(i) Systems development

Many systems which the users feel in their limited knowledge would be useful are developed without adopting any of the standard prescribed procedures. The application while they may be usable immediately, it cannot be assured that they would be maintainable, auditable and securable. Applications like budget preparation, consolidation of accounts, costing, pricing, product-mix decisions are some of the more popular applications which the end-users have developed.

ii. Change controls

As the end-users themselves are developing the programmes the programmes are changed at will without conforming to, again, any established procedures. The fact that the programme with the change implemented has gone live by their own efforts blinds them to the fact that established procedures have been given the go-by.
iii. Data consistency

As mentioned earlier there are data applications which are used in the Finance department, marketing department, manufacturing department as also the costing departments. It is not uncommon to find that there are different versions of the same data being used in the various functional departments. The standard costs as originally developed might have been updated by the costing department but still the old version may continue to be used in the marketing and finance departments while the costing department uses the latest version. This naturally leads to data which is not synchronised and information which is neither reliable nor consistent being provided.

iv. Documentation

Documentation being a cumbersome process and a very limited number of staff being conversant with the usage of computers, it is generally felt that there is no requirement for documentation and the present practices are that there is total absence of documentation regarding the systems and programmes, programme changes and trouble shooting.

v. Software piracy

There is no overall control on the programs that are used at the end-users when the organisation being aware their own departments violate the Copy Rights Acts and are utilising pirated copies of the more popular software.
Back-up and contingency planning for recovery

In the absence of organisation's policies and procedures there is no systematic back-up and recovery procedures, End-users due to lack of technical training are not completely unaware of the need to have adequate back up of data files and programs. In the absence of organisations not having a disaster recovery plan or because end-users are not planned end users do not have adequate contingency planning. It is not uncommon to find end user computing getting interrupted for unusual lengths of time, this necessarily has its own impact on the organisation's operations.

Back-up, at the utmost consists of having copies of programs not necessarily at a remote place. Back-ups if any are generally located in the same area as main storage facility. It is not uncommon to find another floppy box containing data and programs being stored in another drawer of the computer table.

Exposure to virus

Viruses get introduced into the system in any of the following situations.

i. To avoid getting approval to purchase the software unauthorised copies of the software are surreptiously used by the end user. This may result in virus contamination of the entire system.

ii. In the absence of adequate back up and contingency planning attack of a virus does run around program and wipe out files.

The problems were generally the same in all the organisations with End-User computing. Five organisations were selected at random. All the organisations were
large public limited companies which were making use extensively of LOTUS I, II and III and certain simple programs in D-Base. In one organisation, the marketing department was making extensive use of LOTUS I, II and III for pricing decisions. It was found that in view of their being no control procedures there were certain accidental changes to cell values. In addition, in some cases, in view of the software being a pirated copy, the software itself contributed to certain other problems of cell values getting altered without reason. The department staff were programmers, operators-cum-users, all rolled into one. It was a common feature to find alterations being made "ON THE FLIGHT" i.e. even while the software was being used.

In one organisation, a mere crisis situation arose as the single staff in the user department resigned for better prospects. In the absence of documentation and separation of duties and no systematic back up of programs and files, the operations came to a grinding halt.

STANDARD ACCEPTED PROCEDURES

As on many organisations an EUC (End User Computing) represents significant investment, it is essential that it should be properly managed and administered.

The Standard Accepted Procedures could be considered under two heads:

* Control Procedures
* Audit procedures
CONTROL PROCEDURES

Planning

End User Computing should be dealt with like any other business activity. The planning for EUC should address the following areas:

(a) Training organisation should have plans for training personnel on any IT which should cover use of software and hardware and systems development.

Hardware acquisition

Clear guideline should be given regarding the type of hardware to be acquired and the procedure to be followed for such acquisition.

Software

The type of applications to be developed and the method to be adopted for such development. E.g. the language to be used - whether in house development or purchase from vendors.

Utilisation of resources

It is necessary to understand that end users form a part of a whole organisation. Hence there should be coordination and inter-action amongst end users as also the data processing department.
Integration with organisation's business plan

There should be a central department at the corporate level which should decide on the following:

(i) What type of equipment to buy
(ii) Whether to buy the equipment or lease it
(iii) If a networking system is already in existence, whether end user could be provided additional modes.

Designing of appropriate controls in EUC specially in areas where key information is produced to ensure its integrity is essential.

The responsibility of the user with regard to EUC development and integrity and security of data should form part of the overall long term plan of the organisation for IT development. The hardware and software acquisition at EUC should fit into the overall blueprint of the organisation.

Organisational support

Though end user may do its own computing the overall responsibility for its control exists with the organisation. It cannot, under any circumstances, be delegated. The organisation should provide the following:

(i) Guidance

The organisation should have a small group of IT consultants and also an auditor which should provide guidance regarding development of applications as
also clarify any technical doubts. The auditor component of the group should be able
to evaluate the controls of applications in EUC as also its impact on the overall
organisation. The EUC should be provided clear guidance on the following:

* Operational system
* Documentation of systems and programs
* Programs changed procedure
* Data integrity

Responsibility for controls

The ultimate responsibility for the controls in EUC lies with the Head of the
department. They should ensure

(i) Organisational policies and procedures are being adhered to
(ii) Discipline regarding systems development, program changes, operations
etc. are being followed.

To a great extent, controls in EUC environment depend on the effectiveness
of the administrative controls. As the end user has taken on the responsibility of
adhering to the control procedures onus passes on to the end-user.

AUDIT

In view of the extensive growth of EUC specially in view of the significant
benefits that the end user would derive it is necessary for the auditors specially the
internal auditors and subsequently the external auditors to understand the
implications of EUC and its impact on internal controls. The auditors must pay
special attention to the following areas:
(i) Organisational impact of user EUC
(ii) Reasons associated with EUC
(iii) The need for corporate policies and guidelines
(iv) The awareness of management to EUC risks and controls
(v) The procedures being followed in department utilising EUC
(vi) Study of the applications in EUC to evaluate its impact specially on management decision making.

Performing the audit

The auditor should devote his attention to

(i) Controls at organisational level and
(ii) controls at application level

(i) Organisational level

Organisational level he should evaluate the following:
* Administration
* Policies and procedures
* End-user support

Administration

He should study the responsibilities associated with
* Data ownership
* Hardware and software compatibility
* Training
* Technical support
(ii) Policies and procedures

The auditor should evaluate whether there are policies and procedures regarding EUC.

The policies and procedures should cover the following:

* Documentation
* Back up and recovery
* Security
* Hardware acquisition
* Software acquisition
* Development of applications
* Changes to life running programs

End-user support

The End-users need support and the support if any provided should be reviewed to find out whether the following are included:

* Training
* Availability of support.

ANALYSIS AND FINDINGS

Controls

A sample of five organisations at random were chosen and a questionnaire (Table 3.1) was utilised to obtain responses. The practices currently prevalent are as follows:
(a) Segregation of duties is totally absent as the user is a programmer, systems analyst and an operator.

(b) The documentation was totally inadequate if not absent. In their eagerness and enthusiasm to develop systems least importance was given to documentation. The situation did in some cases lead to confusion when the original developer left the department or the organisation. The systems development life cycle procedure has been very rarely followed. There was no feasibility study. No documentation. No test results.

With an attempt at "keeping up with the Jonesses" expensive hardware not justifying the usage of the user department was acquired and remained under utilised.

The systems that are developed did not bear in mind the possible integration with other existing systems or future systems.

"Change control procedures" i.e. the procedures that are needed to be strictly adhered to whenever an existing program is modified or being replaced. Change control procedures were of an inadequate standard. Again, the system was entirely dependent upon the present individual who was using it.

Back up and contingency procedures were not adequate. The back up procedure consisted of a copy of the program being maintained separately in the same room. The usage of unauthorised software was very common. While the organisations might have purchased a licenced software, the end users were having different pirated copies.
The vulnerability for virus was very common. The viruses generally get spread either through the usage of unauthorised copies of software or the floppies which the Maintenance Engineers will be bringing.

AUDIT

Information was gathered from a sample of 30 auditors regarding the procedures they adopt in organisations where End-User computing was in existence and utilised for important areas of operation.

The auditors, either internal or external, were aware of the risks associated with End-User computing environment. There was no audit being performed. The auditors in spite of being aware that Personal Computers were installed in all the functional departments, they were ignorant of the type of applications. The audit in that area was totally absent. Counter-checking of this fact was made with the End-Users who confirmed the same.
### TABLE 3.1

<table>
<thead>
<tr>
<th>Yes / No</th>
</tr>
</thead>
</table>

1. **Organisational**

   Are end-users aware of organisational and departmental information security policies and guidelines?

   Are they adequate and up to date?

   Are computer systems passwords kept confidential by user-employees?

2. **General control**

   Are there policies and guidelines available regarding the following:-

   - Access security
   - Systems Development
   - Change Controls
   - Date consistency
   - Documentation
   - Back-up
   - Recovery
   - Contingency Planning
   - Copyright violation
   - Virus vulnerability
3. **Access security**

Is there a security management function?

Are visitors or unauthorised users having easy access to areas where EUC is performed?

Are files containing sensitive data encrypted?

4. **Systems development**

Are there procedures and controls for systems development?

5. **Change control**

Are there adequate documentation regarding any changes to the programs?

6. **Documentation**

Are there adequate documentation for programs, hardware, system configuration and procedures?

7. **Back-up recovery and contingency**

**Planning :**

Are there procedures and standards for programing and data back-up?

Is there any training provided to End-users regarding dangers of magnetic files static electricity, equipment failure etc.?

If back-up and storage facilities are available, are they in the same area or at a different location?
8. Copy-right violation

Are there written policies informing End-users to the legal consequences of using un-authorised copies of software?

Are there policies and guidelines issued on preventing an attack of virus, debugging it if it is attacked and consequential actions to be taken to nullify the attack of virus?

9. Spread-sheet

Are there specific guidelines given regarding usage of spread-sheet, specially when used for decision-making?
The Institute of Internal Auditors Research Foundation in their "Systems, Auditability and Control" report in Module 7 dealt with End-User and departmental computing. They have conducted a survey and the key survey findings and observations are as follows:

* Forty-one percent of the 249 respondents indicated that one of the highest related risks is poor data accuracy or integrity. Of this 41% (101 respondents), 63% felt the risk would increase in the future, 25% felt there would be no change, and 12% said it would decrease.

* The most effective control mitigate this risk was thought to be policies, standards, and procedures (27%), followed by input/output controls (19%) and systems testing (9%). The respondents citing policies, standards and procedures as the best control indicated that the control is not used in 26% of the organizations, partially used in 70%, and fully used in 4%.

* Other significant risks mentioned included development of incompatible systems and unauthorized access or changes to data or systems. Related controls included policies, standards, and procedures, and access controls and security, respectively.

* Internal audit organizations of all sizes plan to increase audit coverage of EUC over the next three years. Actual coverage in the past three years and planned audit coverage in the next three years are presented in Figure 1.2 for small (one to ten auditors), medium (eleven to sixty auditors) and large (over sixty auditors) internal audit organisations.
Percent of Respondents performing full or limited scope of EUC Audits

<table>
<thead>
<tr>
<th>Audit Coverage</th>
<th>Total Sample</th>
<th>Small (1-10)</th>
<th>Medium (11-60)</th>
<th>Large (61 or more)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual - Past Three Years</td>
<td>71%</td>
<td>57%</td>
<td>71%</td>
<td>85%</td>
</tr>
<tr>
<td>Planned - Next Three Years</td>
<td>91%</td>
<td>84%</td>
<td>91%</td>
<td>99%</td>
</tr>
</tbody>
</table>

SUGGESTIONS

It is advisable to encourage development of End-User Computing in view of the following benefits:

i. Users become self-reliant and hence are more responsive to information needs and requirements.

ii. Application development and maintenance costs are minimal as departmental present needs and future requirements are properly understood.

iii. Back-log of computer applications are considerably reduced as there is clear prioritisation of the department's needs.

It is advisable and hence recommended to take full advantage of the benefits of EUC. Adequate steps need to be taken to avoid associated risks in EUC. The recommended steps would be as follows:

i. Set up a dedicated consulting group within the organisation. It would be advisable to have a small planning cell of competent personnel who would provide the guidance for the end-users. The type of services they would provide include trained end-users generally of traditional systems development as also providing knowledge of general controls and application controls.