Computer Auditing – Control Matters

(Relevant to ATE Paper 8 – Auditing)

David Chow, FCCA, FCPA, CPA (Practising)

The introduction of a computerized or electronic data processing (EDP) accounting system has **not** brought any changes to auditors' audit objectives, i.e. to enable the auditor to express an opinion whether the financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework. However, the methods of applying audit procedures in gathering audit evidence may be influenced by the way accounting data is processed.

Characteristics of Computerized Accounting Systems

Computerized accounting systems have the following characteristics:

(i) Audit trail

A transaction trail that can be used for audit purposes might only exist for a **short period of time** or only be in **computer readable form**. This is because computerized accounting systems eliminate some steps and some documents used that would otherwise be present in manual systems.

(ii) Nature of processing errors

Clerical errors are ordinarily associated with manual processing. In an EDP environment, processing errors are mainly caused by **programming errors** or **systematic errors in the hardware or software**. Furthermore, in computerized systems, data must be converted into machine-readable form; this introduces the possibility of input errors, which are supposed to be detected by input controls.

(iii) Central processing of transactions

When transactions are centrally processed in an EDP department, sometimes many **incompatible functions are combined**. To keep incompatible duties separate, segregation of duties is often established.

(iv) Alteration of data or files

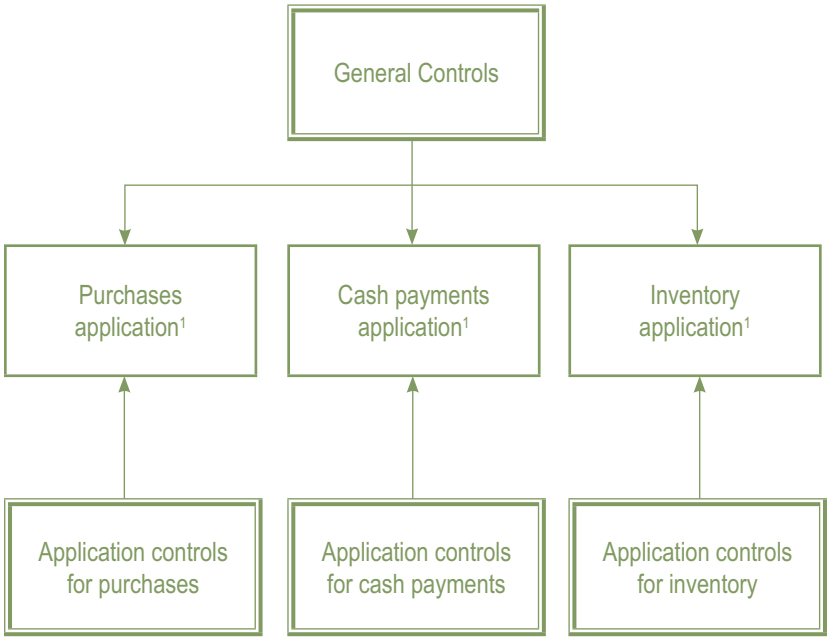
Permanent data (such as a worker's hourly rate) stored in master file can often be **altered without being**

detected; this kind of fraud may not be detected for a long time.

EDP Controls

The control environment in complex EDP systems is even more critical than that in more simple systems because there is greater potential for misstatement. The types of controls in an EDP system are **general controls** and **application controls**. The difference between general and application controls is illustrated in the diagram below, in which three computer applications are shown. General controls affect all three applications, but separate application controls are developed for purchases, cash payments and inventory. Although some application controls affect one or only a few transaction-related audit objectives, most of the procedures prevent or detect several types of misstatements in all phases of the application.

Relationship of General Controls and Application Controls to Audit Applications



1. An application is a programme or group of programmes designed to process a particular group of transactions such as payment of creditors.

General Controls

If general controls are ineffective, there may be potential for material misstatement in each computer-based accounting application.

General controls relate to the **environment** within which systems are developed, maintained and operated. Such controls related to **all parts** of the EDP system and they apply to any one application. Auditors usually evaluate the effectiveness of general controls before evaluating application controls. If general controls are ineffective, there may be potential for material misstatement in each computer-based accounting application. The general controls must therefore be evaluated early in the audit.

General controls are to ensure the **integrity** of application development and implementation and to ensure that computer operations are **properly administered** to protect hardware, programmes and data files. There are five main types of general controls:

(i) Organization of EDP department

No one individual should be able to
(a) access the data;
(b) alter the computer system or programmes; and
(c) access the computer.

There should be **segregation of duties within EDP Department**, so as to prevent EDP personnel from authorizing and recording transactions to hide theft of assets, and to minimize the possibility of recording and processing errors. In principle, no one individual should be able to (a) access the data; (b) alter the computer system or programme, and (c) access the computer.

Suppose that there is inadequate segregation of duties such that computer operators are also programmers and have access to computer programmes and data files, then the auditors would be concerned about the potential for fictitious transactions or unauthorised data and omissions in the accounts.

Assume that the auditors find that there are inadequate safeguards over data files, they may then conclude that there is a significant risk of loss of data because the general controls affect each application.

The following functions should be separated within the EDP Department:

- Applications and programming (design and maintenance of computer hardware and software). It is important that the programmer does not have access to input data on computer operations, since his understanding of the programme can easily be used for personal benefit. The librarian provides a means of important physical control over the computer programmes, transaction files, and other important computer records and releases them only to authorized personnel.
- Operations (running the computer, executing jobs). Ideally, the operator should be prevented from having sufficient knowledge of the programme to modify it immediately before or during its use.
- Data Control (data input and output). The function of the data control group is to test the effectiveness and efficiency of all aspects of the system. This includes the application of various controls, the quality of the input, and the reasonableness of the output.

(ii) Application Development and Maintenance Controls

The purpose of this general control area is to ensure that the client adequately **controls computer programmes and related documentation**. The primary controls are included in the design and use of systems manuals. Documentation is often the best source of information about control features within computer programmes, and thus the auditor's review of computer controls may depend, in part, on adequate documentation. Common types of computer documentation include programme flowcharts and narratives, record and file layouts and operator instructions.

(iii) Hardware Controls

Hardware controls are built into the equipment by the manufacturer to

detect equipment failure. Auditors are less concerned with the adequacy of the hardware controls in the system than with the organization's methods of handling the errors that the computer identifies.

(iv) Access to Computer Equipment, Data Files and Programmes

These general controls are important for **safeguarding EDP equipment and records**. This is accomplished through locked doors, segregation of duties, locked cabinets containing data files, passwords or security codes and reports of jobs run on the computer.

(v) Data or Procedural Controls

Copies of all important files and programmes should be **kept "off site"**. This may prevent losses due to accidental erasure, intentional vandalism, or catastrophic loss (e.g. because of fire). One commonly-used data storage method is the grandfather-father-son method.

Application Controls

Application controls are controls **specific** to a particular accounting application. Separate application controls are developed for different applications. Application controls must be evaluated specifically for every audit area in which the client uses the computer where the auditor plans to reduce assessed control risk.

There are four main types of application controls:

(i) Input controls;
(ii) Processing controls;
(iii) Output controls; and
(iv) Controls over Master File information.

Application controls are to ensure the **completeness and accuracy** of all processing and the **validity** of the accounting entries made. There are four main types of application controls:

(i) Input controls

Controls over input are designed to assure that the information processed by the computer is valid, complete, and accurate. These controls are critical because a large number of errors in computer systems are the results from input errors. Common input controls include check digits, batch totals, hash totals, limits or reasonableness tests, validity checks etc.

(ii) Processing controls

Controls over processing are designed to assure that data input into the system is accurately processed. This means that all data entered in the computer are processed, processed only once, and processed accurately. Most processing controls are also programmed controls, which mean that the computer is programmed to do the checking. Common examples include control totals, logic tests, and completeness tests.

(iii) Output controls

Controls over output are designed to assure that data generated by the computer are valid, accurate, and complete. Moreover, outputs should be distributed in the appropriate quantities only to authorized people. The most important output control is review of the data for reasonableness by someone who knows what the output should look like.

(iv) Controls over Master File information

Many transactions depend on the accuracy of information in the Master File. For example, all sales transactions depend on price list, or all payroll amounts depend on hourly rate or salary rate. User departments should get periodic reports containing the contents of the Master File. There should be procedures in place to verify that the correct version of the Master File is being used.

How do Auditors Test Controls in an EDP Environment?

Auditors obtain information on general and application controls by: (i) **interviewing** EDP staff; (ii) **reviewing flowcharts and documentation** that describe the system and programmes; and (iii) reviewing **internal control questionnaires** they have given the client to complete.

Audit around the computer only when:
(a) the audit trail is complete;
(b) processing operations are straightforward, and
(c) systems documentation is complete and readily available

When the audit trail is incomplete and the computer processing operations are complicated, it is inappropriate to **audit around the computer**. This technique should only be used when the audit trail is complete, computer-processing operations are straightforward and systems documentation is complete and readily available.

Under the technique of auditing around the computer, auditors bypass the computer and treat it as a giant book-keeping machine. This is acceptable in some situations but becomes unacceptable if the relationship between the output and the input cannot be properly understood without examining the intervening computer processing, e.g. when there is no visible audit trail.

Audit through the computer with:
(i) audit test data;
(ii) parallel simulation; and
(iii) integrated test facility

In more complex EDP environments, clients retain data in electronic format only. The loss of audit trail means auditors must test application controls directly by **auditing through the computer**. Auditors test application controls using three types of tests: (i) audit test data, (ii) parallel simulation and (iii) integrated test facility.