Article: Auditing in a computer environment July 2015

Article by Paul Lydon, BA, CPA, MBS (Hons), PGCLTHE, FHEA - Current Examiner in P1 Auditing

Introduction

Whether an auditor is auditing a small company or a large multinational, it is almost certain that information systems will have been used by the client entity in processing financial information (input transactions and accounting records).

The type of accounting software can vary while small companies may use readily available general accounting software that fulfils their requirements, larger companies will often have specific software designed and installed to suit their needs.
In many cases, these software solutions are full enterprise resource planning (ERP) systems. ERP systems are designed to cover all, or the majority of, the core functions of an enterprise, no matter what its business is.

Regardless of the computer systems used, the audit objectives and approach will remain largely unchanged from that if the audit was being carried out in a non-computer environment. These are considered below:

Audit objective — the audit objective will not change, as the auditor must obtain sufficient appropriate audit evidence to draw reasonable conclusions on which to base the audit opinion.

Audit approach - the audit approach will not change as the auditor must continue to plan, ascertain, record and evaluate.

Controls assessment - the requirement for and method of assessing controls will not change, as the normal procedures for control assessment used in a manual system will still exist in a computer controlled environment.

Hence the work undertaken on the financial statements of a company is orchestrated — to enable the auditor determine, whether an organisation's financial statements and financial position are presented fairly in accordance with generally accepted accounting principles (GAAP)

It is important for the auditor to establish facts to their satisfaction as they will be required to report to the members on whether, in their opinion, the company's financial statements give a true and fair view. The auditors' report must be made available to every member and be read at the AGM.

Audit approach in a computerised environment

Auditing around the computer

Historically the auditor wished to ensure that data was correctly input and generated by the computer, this approach is generally referred to as "auditing around the computer". This methodology was primarily focused on ensuring that source documentation was correctly processed and this was verified by checking the output documentation to the source documentation.

Auditing through the computer

Due to the advent of "real time" computer environments, there may only be a limited amount of source documentation or paperwork hence the auditor may employ an approach known as "auditing through the computer". This involves the auditor performing tests on the IT (Information Technology) controls to evaluate their effectiveness.

On completion of the necessary tests, if the auditor is satisfied that the controls are effective, then the auditor may perform a lesser degree of substantive procedures testing.

A high degree of skill and experience often involving IT audit specialists is necessary to undertake such an evaluation of the IT controls. In making the decision to test controls connected to the computer environment, the auditor will consider:

- Extent of Use
- Importance to the Business; and
- Complexity

IT audit and Computer-based audit

The terms "IT audit" and "computer-based audit" are used interchangeably to describe the controls operated by computers but from here on the term IT audit will be used.

Hence when an auditor undertakes an IT audit is undertaken it is to review and evaluate an organisation's information system's availability, confidentiality, and integrity.

This will require the auditor to pose certain questions to ensure:

1. **Availability**
   Potential question - What measures are in place to ensure that the data is available when required?

   To answer this question the auditor will access the organisation's computer system to ensure it will be available for the business at all times when required.

2. **Confidentiality**

   Potential question - What controls are available to ensure that only authorised personnel can access the data?

   The auditor will wish to review and test the confidentiality of the organisation's information to understand that the information in the systems is only disclosed to authorised users.

3. Integrity

Potential question - What controls are in place to prevent unauthorised changes to the data?

Finally the auditor will endeavour to ensure the integrity of the information. This means that the information provided by the system is accurate, reliable, and timely.

The auditor may also need to consider some other key factors which will influence the effective application of controls within the IT system.

Such of these factors include the following:

- Whether processing is centralised or decentralised
- The complexity and level of customisation of the IT system
- The availability of skilled and experienced audit staff.

Once a decision has been made to evaluate IT controls, there are two major types of controls in computerised systems to be considered.

General controls:

- These are controls over the environment in which the computer system is operated. Broadly speaking, this type of control includes:
    - organisational controls
    - systems development controls
    - maintenance controls
    - access controls
    - other general controls

As set out above, the key audit objective when reviewing general IT controls is to ensure that the integrity, availability and confidentiality of the data is appropriately controlled. In order to meet this objective, the auditor will look to identify and test relevant control activities under each of the general control categories as follows:

IT Information Security

In the area of information security the key risks include allowing access to the information by more people than is necessary through a failure to implement appropriately logical security including: user names and passwords, a failure to implement a secure user access management process including a process to approve the setup of new users and to remove access once a person leaves employment. It is also important to ensure that there is an appropriate segregation of duties.

The key controls include:

- implementing logical security tools, such as passwords, firewalls virus protection to govern access;
- appropriate physical and environment security measures are taken; introducing a process to govern the granting and removing of access to the systems, and a process to review access from time to time to ensure that any segregation of duties issues are identified.

IT systems Change Control

The key risks associated with the area of IT change control include the risk that changes are not properly approved by management and that changes are not fully tested so that they deliver their objectives.

The key controls to address these risks include:

- the use of Formal Acquisition and Development Procedures, which **ensure** that before any changes begin they are fully approved by management to ensure that they are in line with the organisation's IT aims and objectives;
- a procedure to ensure that all which is converted from older systems is fully reviewed to ensure that it has been moved correctly;
- controls to restrict access and the ability to make changes so that changes cannot be commenced without approval;
- procedures to ensure that Formal Testing is carried out before the changes are implemented.
- This should include testing by users to ensure that they achieve their aims and by IT to ensure that the changes are correctly developed from a technical point of view.

IT Operations

The main risks in the area of IT operations and interfaces are that all scheduled jobs do not run successfully, that data does not flow accurately from one application to another, that data is not appropriately backed up and that additional or unapproved tasks are run on the systems.

The key controls include:

- a process to monitor all overnight or batch jobs to ensure that these have completed successfully;
- controls to restrict the ability to make changes to scheduled jobs;
- a process to identify and follow up on any jobs which fail to run correctly.

Application controls:

- these are controls designed with the objective of ensuring the accuracy and completeness of:
    - data input controls
    - data processing controls
    - data output controls

Application controls are designed to: (i) detect errors before, during and after the processing of specific types of transaction (ii) to support the IT system controls, and (iii) a sound system of internal control for the entity. Application controls also provide the auditor with the comfort that the recording processing and the reports generated by the computer system are performed properly.

Data Input Controls

Input controls are extremely important as a lot of errors may occur at the input stage. The presence of such controls are designed to ensure that the input data has been authorised correctly, is complete, and accurate. If input errors are detected by the IT system, these need to be reviewed, corrected and resubmitted for inputting into the system again.

These controls include the following:

- Control Totals
- Hash Totals
- Editing Checks
- Key Verification
- Missing Data Check
- Check Digit Verification
- Sequence Check
- Control Totals
- Manual Visual Scanning

Data Processing Controls

Processing controls are designed to provide reasonable assurance that the computer processes have been performed as intended. They ensure that the transactions are not duplicated or lost or improperly changed in any way and that errors are identified and corrected on a timely basis.

These controls include the following:

- Reasonableness Checks
- Find Identification Labels
- Before & After Report
- Control Totals

Data Output Controls

Data output controls are designed to ensure that the processing has been correctly carried out, and the output reports are then distributed to authorised personnel only.

These controls include the following:

- Visual Scanning
- Reconciliation

Cloud computing

Cloud computing as a technology has significantly progressed in commercial computing. One of its key attributes is the ability to distribute computing tasks to a shared pool of resources, which can be accessed quickly with a minimal amount of effort for management.

Cloud computing endeavours to provide easy access to information systems services by combining information systems infrastructure and applications that can be retrieved through/over the Internet. The five essential characteristics of cloud computing are as follows:

- On demand self-service**,** namely availability of cloud services on demand
- Broad network access, services are accessible over the Internet through a range of devices such as laptops, smart phones and tablets etc.
- Resource pooling**,** this allows resources to serve multiple clients, which are configured to meet clients' individual needs.
- Rapid elasticity, the provider can swiftly scale up and rapidly release services and resources.
- Measured service, the use of resources by clients can be monitored, controlled and reported on by the provider.

This article has attempted to introduce a general review of the audit approach in a computerised environment. The reader should consult relevant texts and recommended readings for further details on the different controls mentioned in this article.

Bibliography:

Modern Auditing, 3rd Edition 2008/ Cosserat and Rodda, Wiley.

The Audit Process: Principles, Practice and Cases 6th Edition 2015 Gray, Manson and Crawford, Cengage Learning.

External Auditing and Assurance, An Irish Textbook 2nd Edition 2013, Nolan and Nangle, Chartered Accountants Ireland.