Section 7

IT Controls

Method of Recording Internal Control System

ASJ

- Writing Narrative Notes – NNs
- Preparing & Obtaining Questionnaire – ICQs & ICEQs
- Preparing or obtaining Organogram – Organization Charts
- Preparing Systems Flow Charts – Flow Charts

Levels of Flow Chart

ASJ

Macro

The macro level flowchart is the ‘big-picture’ executive summary of the system. This is sometimes called the ‘Helicopter view’ or 10,000 meters above sea level view.

Mini

The mini level (also called ‘midi’) falls somewhere between big picture macro and fine detail micro. Think of this as the plane flying at 3,000 meters above sea level.

Micro

A micro level flowchart provides the most detail and is useful for analysing the way processes operate. Also called ‘ground level’.

Types of Flow Chart

ASJ

Linear

A linear flowchart displays the sequence of work steps that make up a process. This is invaluable in identifying redundant or unnecessary steps within a process.

Deployment

A deployment flowchart shows the actual process flow and identifies the people or groups involved in each step. A deployment chart shows where the people or groups fit into the process sequence and how they relate to one another throughout the process.

Opportunity

The opportunity flowchart differentiates between:

- **Process activities that add value.**
- **Process activities that add cost only.**

ASJ

Benefits of Flow Chart

- Flowcharts can **enhance auditors' evaluations.**
- The annual updating of a chart is **relatively easy** with additions or deletions.
- A complete flowchart is an **informative description** of the system.
- Showing the various duties performed by one individual also provides **graphic evidence** of any conflicting responsibilities.
- The information is presented in a **logical sense.**
- Flowcharts ensure that a system is recorded in **its entirety.**
- It serves as a **permanent record of a system.**
- It **highlights the strengths and weaknesses** of a system.
- Constructing a flowchart **does not require a person** with high technical expertise.

Limitations of Flow Chart

- These are **only suitable for describing standard systems.**
- Flowcharts are also **not appropriate for recording systems with further classifications** of subsystems or subroutines.
- A flow chart **is a time consuming process** because an auditor must learn about the operating personnel involved in the system and gather samples of relevant documents.
- There is a possibility of **recording and checking areas that are of no audit significance.**
- That flowcharts **are difficult to amend** because a single amendment may require changes in the entire chart.

General & Application Controls

ASJ

General Controls

General IT controls are policies and procedures that relate to many different applications (such as revenue, purchases and payroll). They support the effective functioning of application controls by ensuring the continued proper operation of IT systems.

Application controls

Application controls apply to the processing of individual applications (such as revenue, purchases or payroll). These controls help to ensure that transactions occurred, are authorised and are completely and accurately recorded and processed. These controls could be manual or computerised, depending on the system in question.

Categories of General Controls

- Controls over the **development of new computer information systems** and applications
- Controls over the **documentation and testing of changes** to programs
- The **prevention or detection of unauthorised changes** to programs (for example, by an employee committing fraud.
- Controls to **prevent the use of incorrect data files** or programs.
- Controls to **prevent unauthorised amendments** to data files.
- Controls to **ensure that there will be continuity in computer operations** and that the system will not 'break down' and cease to be operational.

Categories of Application Controls

Authorization controls - All significant transactions are being authorized.

Arithmetic controls - Checking the arithmetic accuracy of records.

Accounting Controls - Maintaining and reviewing accounts and trial balances.

Sequence Controls - Numerical sequence checks.

Exception Controls - Manual follow-up of exception reports

IT Controls - IT controls such as edit checks of input data.

- Input controls
- Processing controls
- Data file controls
- Control over output

Control over Data Transmission

Similar to doctors and lawyers, accountants routinely work with highly confidential client information. They must ensure they comply with the fundamental principle of confidentiality from the accountant's code of ethics.

Controls over data transmission help to ensure data is transmitted both intact (complete and as intended) and also securely without fear of breach of confidentiality.

Controls over data transmission include:

- Programme controls that ensure data is transmitted in the correct format.
- Firewalls to prevent intrusion into the programs that send and receive data.
- Restricting access to source data that is transmitted.
- Only using secured Wi-Fi with password protection.
- Using check sums and check digits to ensure that data received is intact.
- Data encryption

Preventative, Detective & Corrective Controls

ASJ

- **Preventative** - These are controls that prevent the loss or harm from occurring. For example, a control that enforces segregation of responsibilities, minimizes the chance an employee can issue fraudulent payments.

- **Detective** - These controls monitor activity to identify instances where practices or procedures were not followed. For example, a business might review payment request audit logs to identify fraudulent payments.

- **Corrective** - Corrective controls restore the system or process back to the state prior to a harmful event. For example, a business may implement a full restoration of a system from backup tapes after evidence is found that someone has improperly altered the payment data.

ASJ

Logical Access Controls

Logical access controls are protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them.

Logical access controls are typically a system of measures and procedures, both within an organization and in the software products used, aimed at protecting computer resources (data, programs and terminals) against unauthorized access attempts.

In information technology, **logical access controls** are tools and protocols used for identification, authentication, authorization, and accountability in computer information systems.

Logical access is often needed for remote access of hardware and is often contrasted with the term "physical access," which refers to interactions (such as a lock and key) with hardware in the physical environment, where equipment is stored and used.

System Logs

ASJ

A log file is a file that records events taking place in the execution of a system. This generates an audit trail that can be used to understand the activity of the system and to diagnose problems.

Logs are essential for understanding the activities of complex systems and for analysing a system's performance, particularly where there is little user interaction.

Examples of system logs include:

- Which user logged-in, when and where from.
- Failed log-in attempts.
- Who accessed and amended data in a file.
- Changes made to a program – what, when and by whom.
- When employees entered and left the building.
- Black box flight recorders.
- CPU speed.
- Broadband speed.
- Which web pages a user accessed.
- Attempted cyber intrusions