ජයසේකර කළමනාකරණ මධ්‍යස්ථානය
JMC JAYASEKERA MANAGEMENT CENTRE (PVT) LTD Estd. 1972
"Pioneers in Professional Education"

# ADVANCED AUDIT AND ASSURANCE

# CORPORATE LEVEL

# TUTE 15

# INTERNAL CONTROLS IN COMPUTERIZED ENVIRORMENT & DIGITALIZATION IN AUDIT PROCESS

by

Jeewantha Perera

(FCA, ACCA, MBA, B.Sc Accountancy (sp)

# INTERNAL CONTROLS IN A COMPUTERISED ENVIRONMENT

There are special considerations for auditors when a system is computerised. In controls comprise general and application controls. The internal controls in a computerised environment include both manual procedures and procedures designed into computer programs. Such control procedures comprise two types of control: **General Controls and Application Controls**.

## General Controls

General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls by helping to ensure the continued proper operation of information systems. The purpose of the General IT controls is to establish a framework of overall control over the computer information system activities to provide a reasonable level of assurance that the overall objectives of internal controls are achieved.

| **General Control Type** | **Example** |
|---|---|
| Development of Computer Applications | Segregation of duties so that those responsible for design are not responsible for testing |
| | Obtaining proper approval from the Computer Users and Management before performing system modifications and document all the changes performed |
| | Providing proper training to staff |
| | |
| Prevention or Detection of Unauthorized Changes to the Programmes | User Identification Controls such as Password protections |
| | Restricted access to the Central Computer Systems |
| | Obtaining backups of the Computer Programme |
| | |
| Controls to Prevent Unauthorized Amendments to Data Files | User Identification Controls such as Password protections |
| | Firewalls |
| | Obtaining backups of the Data files |
| | |
| Testing and Documentation of Programme Changes | Obtaining proper approval from the Computer Users and Management before performing system modifications and document all the changes performed |
| | Providing proper training to staff |
| | |
| Controls to Ensure Continuity of Operations | Storing extra copies of programmes and data files off -site |
| | Protection of Equipment’s against fire and other hazards |
| | Disaster Recovery Procedures |

## Application Controls.

Application controls are manual or automated procedures that typically operate at a business process level. They can be preventative or detective in nature and are designed to ensure the integrity of the accounting records. Accordingly, they relate to procedures used to initiate, record, process and report transactions or other financial data.

The purpose of application controls is to establish specific control procedures over accounting applications in order to provide reasonable assurance that all transactions are authorized and recorded, and are processed completely, accurately and on a timely basis.

**A) Input Controls**

Input Controls are mainly focussing on Accounting Input such as transactions and events.

Eg: Manual checks to ensure information input is authorized
System checks to ensure information input is authorized
Continuity Check
Completeness Check

**B) Processing Controls**

These are the controls applicable in the processing stage, such as recording, categorizing, analysing of transactions and events

Eg: Consistency Check
Completeness Check

**C) Output Controls**

These are the controls applicable to the output of the Accounting System which is Financial Statements

Eg: Preparation of Bank Reconciliations
Recalculations to check the accuracy of the output – Depreciation
Preparation of Control Accounts

Internal controls in IT systems are essential to provide reasonable assurance that IT systems will function as intended and fulfil their purpose effectively.

1. Many general IT controls are procedural in nature. They help to create risk awareness in all IT applications. They are also necessary to ensure that IT applications are implemented with limited risks.

2. Application controls are largely controls written into the application software, to check for errors, and report (or automatically correct) errors that are detected.

## Additional Notes

# DIGITALIZATION IN AUDIT PROCESS

## INTRODUCTION

Digital business is revolutionising the commercial environment by reducing the distinction between businesses and processes in the digital world and the real world.

Key Areas

A) Artificial intelligence (Al) refers to machines or computers completing tasks that require human intelligence. AI is programmes or software applications which replaces the human intelligence with computer applications.
Eg: Siri in apple I phones.

B) Robotic process automation (RPA) is the use of software to complete rules-based tasks more efficiently than is possible using manual processes. It means robotic software and applications are replacing repetitive tasks, which were earlier performed by humans
Eg: Preparation of bank reconciliation rather than having the manual interventions.

C) Block chain - It is a process of stored the data in a digitally corded block. Block Chains are digitally coded box of information, where data is stored. It is highly transparent due to fact of viewing access is being available to any stakeholders. However, changes can be done by individuals having access to data.
Eg : In Financial Reporting, ledger of a business organization can be stored as a block chain where the required parties can review it.

D) Fin Tech (Financial Technology) - Fin Tech is a technology where digital technology facilitating financial transactions. Eg: E volet, electronic money, mobile banking applications.

E) Big Data - is a broad term for the larger, more complex datasets that can be held by modern computers. The term refers to a qualitative shift in the amount of data that is available in comparison with the past.

F) Data analytics is the examination of data to try to identify patterns, trends or correlations. As the quantity of data has increased, it has become more and more necessary to evolve ways of processing and making sense of it. In Auditing Data Analytics can be used to perform Analytical Procedures in Risk Assessment

## AUDIT AUTOMATION RESULTED FROM DIGITALIZATION.

Audit automation, through the use of data analytics, makes it possible to test 100% of transactions and improve efficiency. Therefore, most of the Audit Firms are using Audit Data Analytics (ADA) tools to perform the procedures.

## COMPUTER ASSISTED AUDITING TECHNIQUES

Computer assisted audit techniques (CAATs) are the use of computers for audit work. The two most used CAATs are ***audit software*** and ***test data***. Computer assisted audit techniques (CAATs) are the applications of auditing procedures using the computer as an audit tool.

The advantages of using CAATs are:

- Auditors can test programme/application controls as well as general internal controls associated with computers.
- Auditors can test a greater number of items more quickly and accurately than would be the case otherwise.
- Auditors can test transactions rather than paper records of transactions that could be incorrect.
- CAATs are cost-effective in the long term if the client does not change its systems.
- Results from CATs can be compared with results from traditional testing

The disadvantages associated with using CAATs include:

- Setting up the software needed for CAATs can be time consuming and expensive
- Audit staff will need to be trained so they have a sufficient level of IT knowledge to apply CAATs
- Not all client systems will be compatible with the software used with CAATS
- There is a risk that live client data is corrupted and lost during the use of CAATS

The major steps to be undertaken by the auditors in the application of a CAAT are as follows.

- Set the objective of the CAAT application
- Determine the content and accessibility of the entity's files
- Define the transaction types to be tested
- Define the procedures to be performed on the data
- Define the output requirements
- Identify the audit and computer personnel who may participate in the design and application of the CAAT
- Refine the estimates of costs and benefits
- Ensure that the use of the CAAT is properly controlled and documented
- Arrange the administrative activities, including the necessary skills and computer facilities
- Execute the CAAT application
- Evaluate the results

## AUDIT SOFTWARE

Audit software consists of computer programs used by the auditors, as part of their auditing procedures, to process data of audit significance from the entity's accounting system. It may consist of generalised audit software or custom audit software. ***Audit software is used for substantive procedures.***

Audit software's are computer software that are being used by the auditors to perform audit procedures. Audit software performs tasks such as,

a) Extracting data from computer files
b) Reading Data from files
c) Selecting Samples

Audit software's can be divided into two types

A) Generalised Audit Software which can be used for multiple purposes
B) Custom Audit Software's, which can be used for specific tasks

Generalised audit software allows auditors to perform tests on computer files and databases, such as reading and extracting data from a client's systems for further testing, selecting data that meets certain criteria, performing arithmetical calculations on data, facilitating audit sampling and producing documents and reports.

Custom audit software is written by auditors for specific tasks when generalised audit software cannot be used.

## BENEFITS OF USING AUDIT SOFTWARE

1. Audit software can perform calculations and comparisons more quickly than those done manually.

2. Audit software makes it possible to test more transactions

3. Audit software may allow the actual computer files (the source files) to be tested from the originating program

## DISADVANTAGES OF USING THE AUDIT SOFTWARE

1 The costs of designing tests using audit software can be substantial, as a great deal of planning time will be needed in order to gain an in-depth understanding of the client's systems so that appropriate software can be produced

2 The audit costs in general may increase, because experienced and specially trained staff will be required to design the software, perform the testing and review the results of the testing.

3 If audit software has been designed to carry out procedures during live running of the client's system, there is a risk that this disrupts the client's systems.

## TEST DATA

Test data techniques are used in conducting audit procedures by entering data (eg a sample of transactions) into an entity's computer system, and comparing the results obtained with pre-determined results. Test data is used for tests of controls.

## CLOUD BASED AUDIT WORKING PAPERS

Cloud based audit working papers are generated through the use of cloud-based software that enables collaboration between the audit team and efficient management of working papers.

Cloud based software can be used by the auditor to manage the audit process and to generate audit working papers which are then stored safely and securely online.

The cloud based nature of the software means that the audit data is always accessible and is always backed up, thereby reducing the risk of loss of data. Real-time dashboards are available that enable audit managers to quickly assess the status of the audit and take corrective action where problems arise. The integration of up-to-date auditing standards and requirements means that compliance is made easier for the audit firm.

The accessibility of the working papers is enhanced in a cloud-based system as It will be accessible in any location on any device and is usually supported by smartphones, laptop and tablets as well as desktop computers.

## CYBER SECURITY

Organisations require controls to reduce the risk of cyber attacks on their systems or unauthorised access

Cyber risks are risks that arise from holding customer data, intellectual property or digital information that may be of use or value to cyber criminals.

Cyber controls are controls that an organisation should put in place to minimise cyber risk and prevent loss of data or unauthorised access.

### Cyber Security Risk

In todays fast-moving digital environment, it is important that organisations have in place sufficient controls to mitigate the risk related to cyber attacks. Such attacks have the potential to disrupt business, cause major reputational risk, and potentially lead to legal action against the organisation.

Whilst the risk around cyber security is high, there are controls that companies and senior managers can implement to reduce the risk.

As a result of the dynamic nature of the digital environment, the most important aspect of cyber security is to have a risk management process in place to identify and quantify the risks in the first place.

| | Cyber Security Risk | Nature | Controls to Mitigate the Risk |
|---|---|---|---|
| 01 | Data Hacking | Hackers gaining access to IT systems from outside the organization and steal data | All networks to be protected by Firewalls |
| | | | Access Restrictions among employees |
| | | | All user accounts to be protected by Password and User Names |
| | | | |
| 02 | Insider Treats | Mistaken or malicious leaking of Data by employees | Limiting staff access to the system |
| | | | Restrict use of portable storage devices |
| | | | Immediate removal of access for employees who leave the Company |
| | | | |

| | | | |
|---|---|---|---|
| 03 | Data Leakages | Use of Smart Phones and Tablets to deliver threats onto the network or for theft data | Restrict the use of personal devices on the Company Networks<br>Discourage employees from using Company devices on third party networks such as Internet Café's<br>Installation of Anti-Virus Software and regular upgrades |
| | | | |
| 04 | C | Loss of Data or introduction of threats via external data storage devices | Restrict all such devices to those owned and purchased by Company<br>Scan all those external devices with Anti-Malware software each time those are connected to the internal systems |
| | | | |
| 05 | Ransomware and Malware | Mostly delivered via email, it encrypts data and demand a ransom for its release | Installation of anti-virus software and Malware projection software<br>Installation of Firewalls to manage inward and outward communications<br>Raising awareness among employees<br>Regular upgrading of operating systems and software<br>Obtaining regular back-ups |

**Recovery planning**

It is very difficult to make any system 100% secure and as such, companies should have a plan in place to deal with a security breach a situation that leads to an inability to serve customers' needs for a period of time.

There should be procedures in place to identify at an early stage whether there is a problem and to enable preventative action to be taken. IT specialists should be made aware as soon as possible, and a contact list for those involved in addressing any issues kept updated and off site.

Consideration should be given to how business continuity would be maintained in the event of critical systems being made unavailable for a period of time, and regular back-ups made that are easily available but saved off-site.

Those who would be involved in such a situation should be trained and the plan laid out in a document with access restricted to those individuals and to the risk management team.

.