CHAPTER 6

AUDIT IN AN AUTOMATED ENVIRONMENT

LEARNING OUTCOMES

After studing this chapter, you will be able to:

- Understand the meaning of an Automated environment.
- Understand the relevance of IT in an audit.
- Learn how to perform an understanding of an Automated environment and documenting the same.
- Identify the various risks in Automated environment and the corresponding controls.
- Gain knowledge of internal financial controls as per regulatory requirements.
- Recognize the way data analytics can be used in an audit.
- Learn to assess and report audit findings.

CHAPTER OVERVIEW

With the increasing adoption of information technology, business today rely on software systems and applications more than ever. Many of these IT systems generate and process data that is used in the preparation of financial statements of a company. The auditors also often rely on the data and reports that are generated from these systems. In this context, it is critical to understand the IT specific risks that could potentially impact the integrity and reliability of financial transactions and data flowing through a company's systems.

In this chapter, we will learn about the need, relevance and approach to be adopted when performing an audit in an Automated environment that is driven by IT systems and applications that are used in the preparation of financial statements of a company. We will see how the work performed with respect to Automated environment fits into the overall financial statement audit process. We will also understand how data analytics can become useful in an audit.

Finally, we will look at how to assess audit findings and report them to the stakeholders.

1. WHAT IS AN AUTOMATED ENVIRONMENT?

Let us first understand what the term "Automated Environment" means. An automated environment basically refers to a business environment where the processes, operations, accounting and even decisions are carried out by using computer systems – also known as Information Systems (IS) or Information Technology (IT) systems. Nowadays, it is very common to see computer systems being used in almost every type of business.

Example

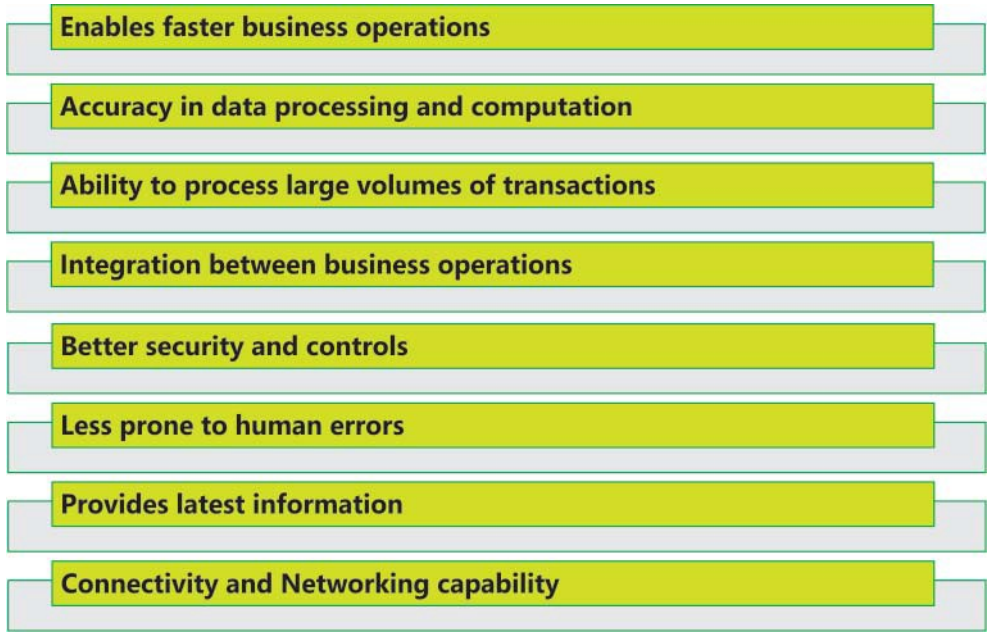
Think about how banking transactions are carried out using ATMs (Automated Teller Machines), or how tickets can be purchased using "apps" on mobile phones, etc. In these examples, you can see how these computer systems enable us to transact business at any time and any day.

Some of the key features of an automated environment are as follows:

1.1 Key features of an Automated Environment

The fundamental principle of an automated environment is the ability to carry out business with less manual intervention and more system driven. The complexity of a business environment depends on the level of automation i.e., if a business

environment is more automated, it is likely to be more complex.



If a company uses an integrated enterprise resource planning system (ERP) viz., SAP, Oracle etc., then it is considered more complex to audit. On the other hand, if a company is using an off-the-shelf accounting software, then it is likely to be less automated and hence less complex environment.

Example

Similarly, there are several other aspects that an auditor should consider to determine the level of automation and complexity of a business environment which we will look at in the following sections.

2. RELEVANCE OF 'IT' IN AN AUDIT

When a business operates in a more automated environment it is likely that we will see several business functions and activities happening within the systems. Consider the following aspects instead of:

- Computation and Calculations are automatically carried out (for example, bank interest computation and inventory valuation).
- Accounting entries are posted automatically (for example, sub-ledger to GL postings are automatic).

- Business policies and procedures, including internal controls, are applied automatically (for example, delegation of authority for journal approvals, customer credit limit checks are performed automatically).
- Reports used in business are produced from systems. Management and other stakeholders rely on these reports and information produced (for example, debtors ageing report).
- User access and security are controlled by assigning system roles to users (**for example,** segregation of duties can be enforced effectively).

Companies derive benefit from the use of IT systems as an enabler to support various business operations and activities. Auditors need to understand the relevance of these IT systems to an audit of financial statements.

While it is true that the use of IT systems and automation benefit the business by making operations more accurate, reliable, effective and efficient, such systems also introduce certain new risks, including IT specific risks, which need to be considered, assessed and addressed by management.

To the extent that it is relevant to an audit of financial statements, even auditors are required to understand, assess and respond to such risks that arise from the use of IT systems.

[Note: Students may refer SA 315 – Identifying and assessing the risks of material misstatement through understanding the entity and its environment for detailed understanding]

In an audit of financial statements, the primary focus is around those risks that are relevant to financial reporting. However, there could be other non-audit assurance engagements that auditors maybe involved wherein the area of focus could include those IT risks relevant to company's compliance and business operations in addition to financial reporting risks.

Examples of such non-audit assurance engagements are internal audits, IT audits, pre-implementation reviews, data migration audits, third party assurance.

With the introduction of the Companies Act 2013, there is greater emphasis given to internal financial controls (IFC) from a regulatory point of view. Directors and those charged with governance (including Board of directors, Audit committee) are responsible for the implementation of internal controls framework within the company. The auditors' responsibilities now include reporting on Internal Financial Controls over Financial Reporting which include and understanding IT environment of the company and relevant risks & controls. We will learn more about IFC in

further sections of this chapter.

Given below are some situations in which IT will be relevant to an audit,

- Increased use of Systems and Application software in Business (for example, use of ERPs)
- Complexity of transactions has increased (multiple systems, network of systems)
- Hi-tech nature of business (Telecom, e-Commerce).
- Volume of transactions are high (Insurance, Banking, Railways ticketing).
- Company Policy (Compliance).
- Regulatory requirements - Companies Act 2013 IFC, IT Act 2008.
- Required by Indian and International Standards - ISO, PCI-DSS, SA 315, SOC, ISAE.
- Increases efficiency and effectiveness of audit.

In some of the above situations it is likely that carrying out audit using traditional substantive audit procedures may be difficult or even not feasible if the company prepares, records and conducts majority of business activities through IT systems only.

On the other hand, many companies may use less complex IT systems including desktop based accounting or spreadsheets. In such situations, the relevance of IT to an audit could be less. However, the auditor is still required to carry out at least an understanding the IT environment of the company and document the same.

Another area where IT can be relevant to audit is by using data analytics using computer assisted audit techniques (CAATs). By using data analytics, it is possible to improve the effectiveness and efficiency of an audit. We will learn more about data analytics in the later sections of this chapter.

From the above, we can see how IT is relevant to an audit under different situations viz., audit, non-audit and meeting regulatory compliance requirements. We will learn more about understanding risks, controls and documentation in further sections of this chapter.

3. RISKS & CONTROLS IN AN AUTOMATED ENVIRONMENT

3.1 Understanding and Documenting Automated Environment

In the previous section, we have learnt that, in an audit of financial statements, an auditor is required to understand the entity and its business, including IT as per SA 315. Understanding the entity and its automated environment involves understanding how IT department is organised, IT activities, the IT dependencies, relevant risks and controls.

Given below are some of the points that an auditor should consider to obtain an understanding of the company's automated environment:

- Information systems being used (one or more application systems and what they are).
- Their purpose (financial and non-financial).
- Location of IT systems - local vs global.
- Architecture (desktop based, client-server, web application, cloud based).
- Version (functions and risks could vary in different versions of same application).
- Interfaces within systems (in case multiple systems exist).
- In-house vs Packaged.
- Outsourced activities (IT maintenance and support).
- Key persons (CIO, CISO, Administrators).

The understanding of a company's IT environment that is obtained should be documented [Ref. SA 230 – *Audit Documentation*] using any standard format or template.

An example of one such template that can be used to document our understanding is illustrated below.

Information Systems being used	Verion	Purpose	Location-Local vs global	Architecture	Interfaces within systems	In-House vs. Packaged	Outsourced Activities	Key Persons	In-Scope
SAP	ECC 6.0, EHPS	Accounting, Supply chain, Production	Texas, USA	Client/Server, Unix AIX 5.3, MS-SQL Server 2008	Paymaster	Packaged		CIO, Administrators	Yes

PayMaster	5.3	Payroll	Gurgaon, India	Web-based, Windows, Apache, Oracle 11g	SAP, Accent	Packaged	Payroll processed at ADP		Yes
Accent	2	Appraisal	Hyderabad, India	Lotus Notes, Windows	Paymaster	In-house			No
Budget King	1	Management MIS Budgeting	Hyderabad, India	Web-based, Windows, Apache, Oracle 11 g	None	In-house			No

Having a summarized document helps the auditor in determining the areas considered in scope of audit as can be seen from the last column. In this illustration, it can be seen that two applications have been considered as in scope for audit based on the purpose and financial relevance to the audit.

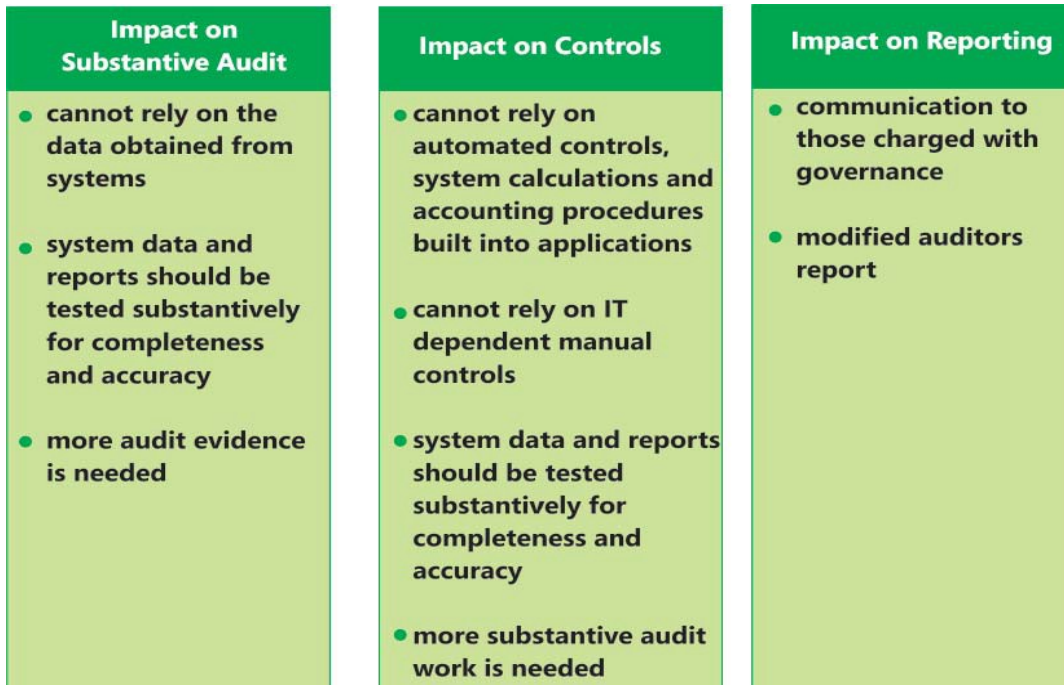
Having obtained an understanding of the IT systems and the automated environment of a company, the auditor should now understand the risks that arise from the use of IT systems.

Given below are some such risks that should be considered:

- Inaccurate processing of data, processing inaccurate data, or both.
- Unauthorized access to data.
- Direct data changes (backend changes).
- Excessive access / Privileged access (super users).
- Lack of adequate segregation of duties.
- Unauthorized changes to systems or programs.
- Failure to make necessary changes to systems or programs.
- Loss of data.

3.2 Impact of IT related risks i.e. on Substantive Audit, Controls and Reporting

The above risks, if not mitigated, could have an impact on audit in different ways. Let us understand how:



- First, we may not be able to rely on the data obtained from systems where such risks exist. This means, all forms of data, information or reports that we obtain from systems for the purpose of audit has to be thoroughly tested and corroborated for completeness and accuracy.
- Second, we will not be able to rely on automated controls, calculations, accounting procedures that are built into the applications. Additional audit work may be required in this case.
- Third, due to the regulatory requirement of auditors to report on internal financial controls of a company, the audit report also may have to be modified in some instances.

In all the above scenarios, it is likely that the auditor will be required to obtain more audit evidence and perform additional audit work. The auditor should also be able to demonstrate how the risks were identified and what audit evidence was obtained and validated to address these IT risks.

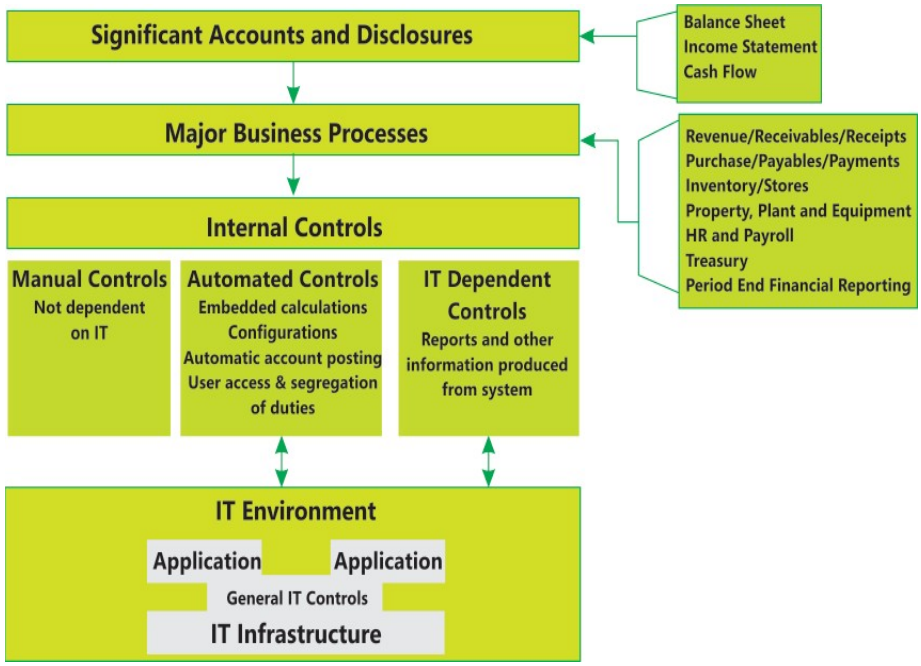
Here, we should remember that as the complexity, automation and dependence of business operations on IT systems increases, the severity and impact of IT risks too increases accordingly. The auditor should apply professional judgement in determining and assessing such risks and plan the audit response appropriately.

To mitigate the above (and more) risks and maintain the confidentiality, integrity,

availability and security of data, companies implement IT controls. Let us learn about the various types of IT controls in more detail.

3.3 Types of Controls in an Automated Environment

- General IT Controls
- Application Controls
- IT-Dependent Controls



3.3.1 General IT Controls

"General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, miniframe, and end-user environments.

General IT-controls that maintain the **integrity** of information and **security of data** commonly include controls over the following:" (SA 315)

- Data center and network operations
- Program change
- Access security
- Application system acquisition, development, and maintenance (Business Applications)

These are IT controls generally implemented to mitigate the IT specific risks and applied commonly across multiple IT systems, applications and business processes. Hence, General IT controls are known as "pervasive" controls or "indirect" controls. Let us now learn about each of the General IT controls in more detail.

Data Center and Network Operations

Objective: To ensure that production systems are processed to meet financial reporting objectives.

Activities:

- Overall Management of Computer Operations Activities
- Batch jobs – preparing, scheduling and executing
- Backups – monitoring, storage & retention
- Performance Monitoring – operating system, database and networks
- Recovery from Failures – BCP, DRP
- Help Desk Functions – recording, monitoring & tracking
- Service Level Agreements – monitoring & compliance
- Documentation – operations manuals, service reports

Program Change

Objective: To ensure that modified systems continue to meet financial reporting objectives.

Activities:

- Change Management Process – definition, roles & responsibilities
- Change Requests – record, manage, track
- Making Changes – analyze, design, develop
- Test Changes – test plan, test cases, UAT
- Apply Changes in Production
- Emergency & Minor Changes
- Documentation – user/technical manuals
- User Training

Access Security

Objective: To ensure that access to programs and data is authenticated and authorized to meet financial reporting objectives.

Activities:

- Security Organization & Management
- Security Policies & Procedures
- Application Security
- Data Security
- Operating System Security
- Network Security – internal network, perimeter network
- Physical Security – access controls, environment controls
- System Administration & Privileged Accounts – Sysadmins, DBAs, Super users

Application system acquisition, development, and maintenance

Objective: To ensure that systems are developed, configured and implemented to meet financial reporting objectives.

Activities:

- Overall Mgmt. of Development Activities
- Project Initiation
- Analysis & Design
- Construction
- Testing & Quality Assurance
- Data Conversion
- Go-Live Decision
- Documentation & Training

3.3.2 Application Controls

Application controls include both automated or manual controls that operate at a business process level. Automated Application controls are embedded into IT applications viz., ERPs and help in ensuring the completeness, accuracy and integrity of data in those systems.

Examples of automated applications include edit checks and validation of input data, sequence number checks, user limit checks, reasonableness checks, mandatory data fields.

3.3.3 IT dependent Controls

IT dependent controls are basically manual controls that make use of some form of data or information or report produced from IT systems and applications. In this case, even though the control is performed manually, the design and effectiveness of such controls depends on the reliability of source data.

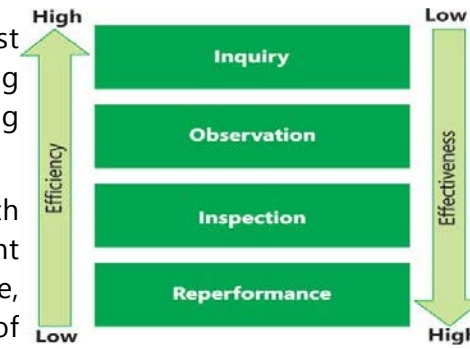
Due to the inherent dependency on IT, the effectiveness and reliability of Automated application controls and IT dependent controls require the General IT Controls to be effective.

3.3.4 General IT Controls vs. Application Controls

- These two categories of control over IT systems are interrelated.
- The relationship between the application controls and the General IT Controls is such that General IT Controls are needed to support the functioning of application controls, and both are needed to ensure complete and accurate information processing through IT systems.

4. TESTING METHODS

Having learnt about the various IT risks and controls, let us understand the different ways testing is performed in an automated environment. There are basically four types of audit tests that should be used. They are inquiry, observation, inspection and reperformance. As shown in the illustration below, inquiry is the most efficient audit test but it is also gives the least audit evidence. Hence, inquiry should always be used in combination with any one of the other audit testing methods. Inquiry alone is not sufficient.



Reperformance is most effective as an audit test and gives the best audit evidence. However, testing by reperformance could be very time consuming and least efficient most of the time.

Generally, applying inquiry in combination with inspection gives the most effective and efficient audit evidence. However, which audit test to use, when and in what combination is a matter of professional judgement and will vary depending on several factors including risk

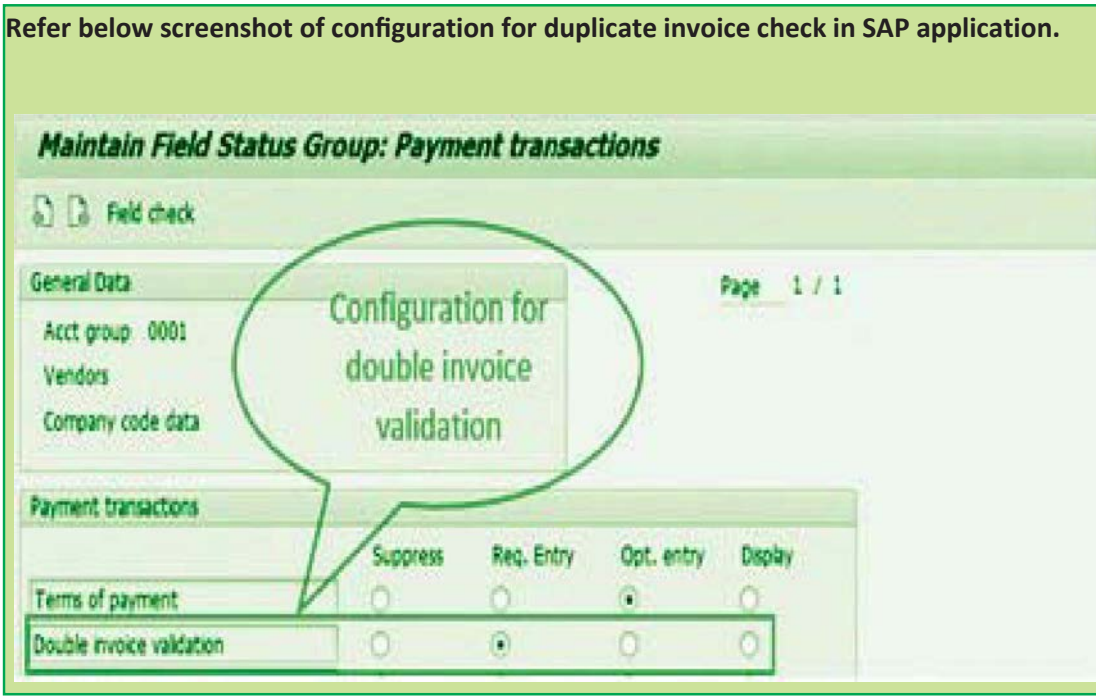
assessment, control environment, desired level of evidence required, history of errors/misstatements, complexity of business, assertions being addressed, etc. The auditor should document the nature of test (or combination of tests) applied along with the judgements in the audit file as required by SA 230.

When testing in an automated environment, some of the more common methods are as follows:

- Obtain an understanding of how an automated transaction is processed by doing a walkthrough of one end-to-end transaction using a combination of inquiry, observation and inspection.
- Observe how a user processes transactions under different scenarios.
- Inspect the configuration defined in an application.

Example

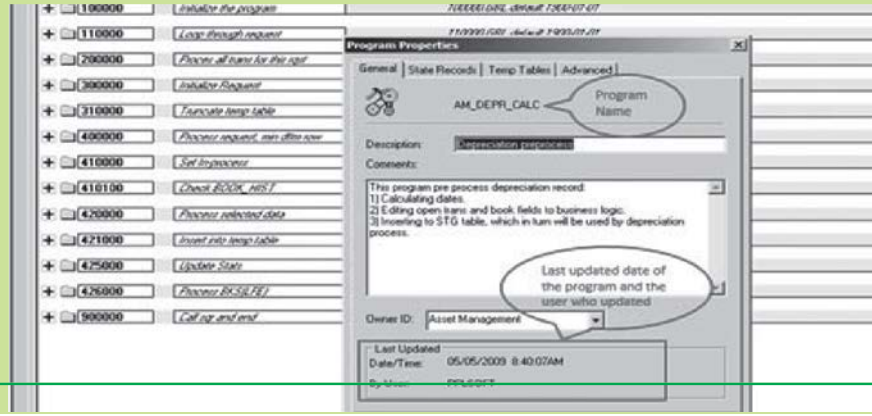
Refer below screenshot of configuration for duplicate invoice check in SAP application.



- Inspect the system logs to determine any changes made since last audit testing.

Example

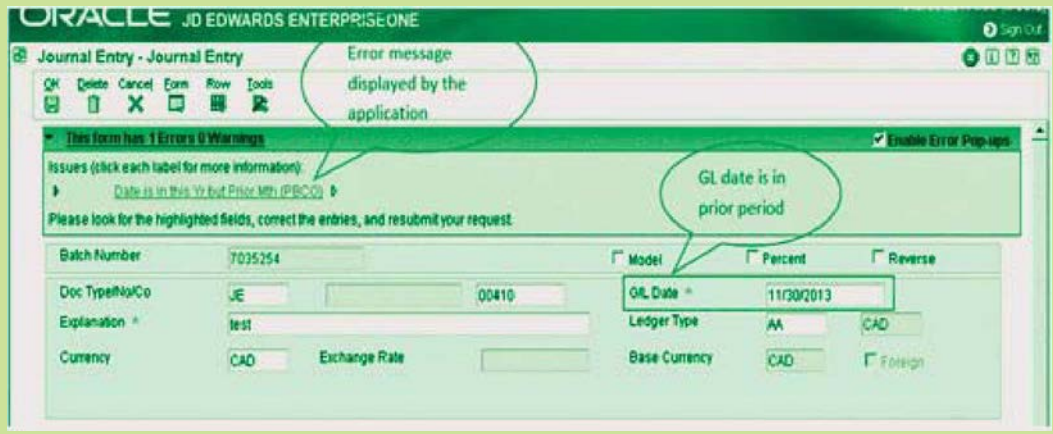
For example, refer below screenshot for the last modified date of depreciation calculation program in PeopleSoft application



- Inspect technical manual / user manual of systems and applications.
- Carry out a test check (negative testing) and observe the error message displayed by the application.

Example

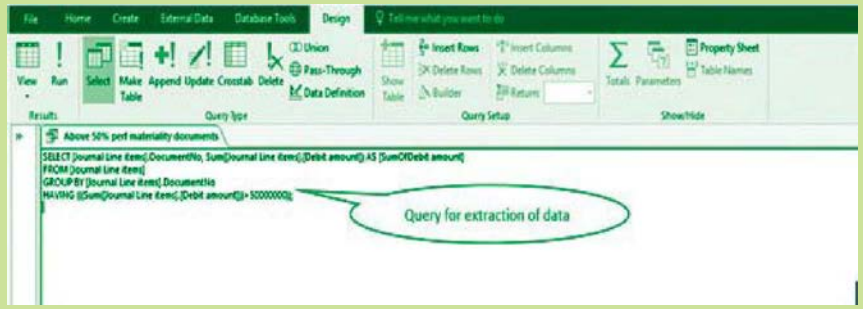
See below an error displayed by an application i.e. JD Edwards, when posting a transaction in closed period.



Conduct reperformance using raw source data and independently applying formulae, business rules or validations on the source data using CAATs.

Example

Refer below the screenshot of a query in MS Access for extraction of journal entries for above rupees 5 crores.



To rely on the system and application based information including data, reports, automated controls, configurations, calculations and IT dependent it is essential to first determine the existence and effectiveness of General IT Controls **[ref para 3.3 above].** Where the general IT controls are not existing or existing but ineffective, the auditor should assess the impact of IT risks and complexity of the automated environment in which the business operations take place and plan alternative audit procedures in order to rely on the system based information **[ref para 3.2 above**].

5. INTERNAL FINANCIAL CONTROLS AS PER REGULATORY REQUIREMENTS

The term **Internal Financial Controls (IFC)** basically refers to the policies and procedures put in place by companies for ensuring:

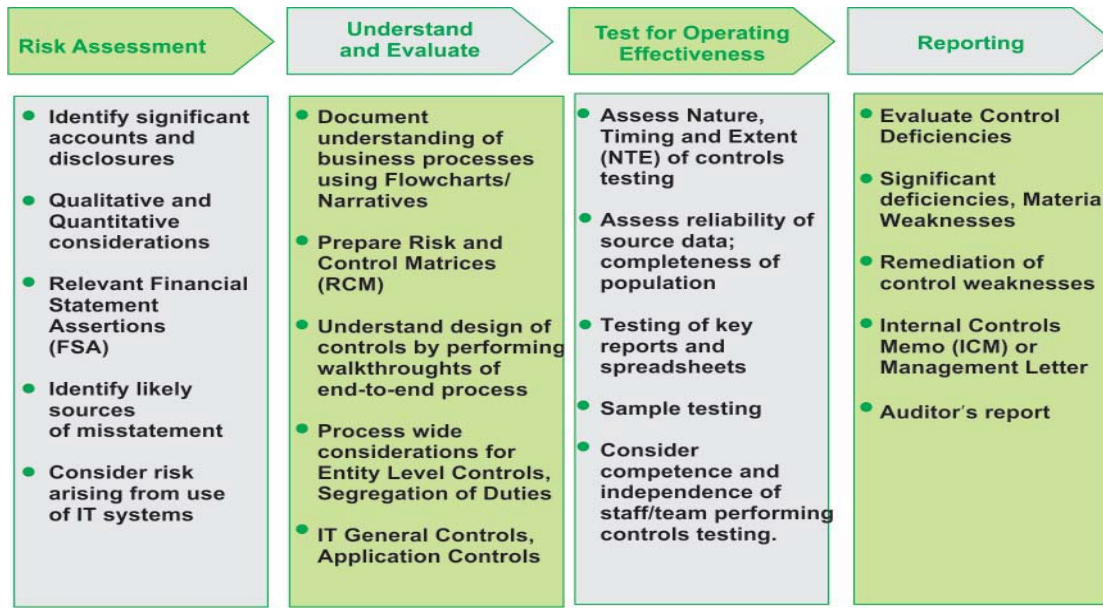
- reliability of financial reporting
- effectiveness and efficiency of operations
- compliance with applicable laws and regulations
- safeguarding of assets
- prevention and detection of frauds

The Companies Act, 2013 has placed a greater emphasis on the effective implementation and reporting on the internal controls for a company. The table below gives a summary of the requirements of the Act.

Reference	Who is responsible	Applicability
Sec 134(5)(e)	Board of Directors	Listed Companies*
Rule 8 (5) of Companies (Accounts) Rules	Board of Directors	All Companies
Sec 149(8) and Schedule IV	Independent Directors	All companies having Independent Directors
Sec 177	Audit Committee	All companies having Audit committee
Sec 143(3) (i)	Statutory Auditors	All Companies#

* IFC is applicable from April 1, 2014 onwards, for companies.
# Auditor's opinion on IFC is applicable from the financial year 2015-16 onwards wherein the Statutory Auditors, along with their opinion on financial statements, should also provide an Independent Opinion on the Design and Operating Effectiveness of Internal Financial Controls over Financial Reporting (IFC-FR) of the company as at Balance Sheet date.

The directors and management have primary responsibility of implementing and maintaining an effective internal controls framework and auditors are expected to evaluate, validate and report on the design and operating effectiveness of internal financial controls. The Guidance note on Audit of Internal Financial Controls over Financial Reporting issued by the Institute of Chartered Accountants of India provides a framework that auditors should follow to fulfil their responsibility. The below illustration is a summary of this controls based audit approach.



5.1 Audit Approach

6. DATA ANALYTICS FOR AUDIT

In today's digital age when companies rely on more and more on IT systems and networks to operate business, the amount of data and information that exists in these systems is enormous. A famous businessman recently said, "Data is the new Oil".

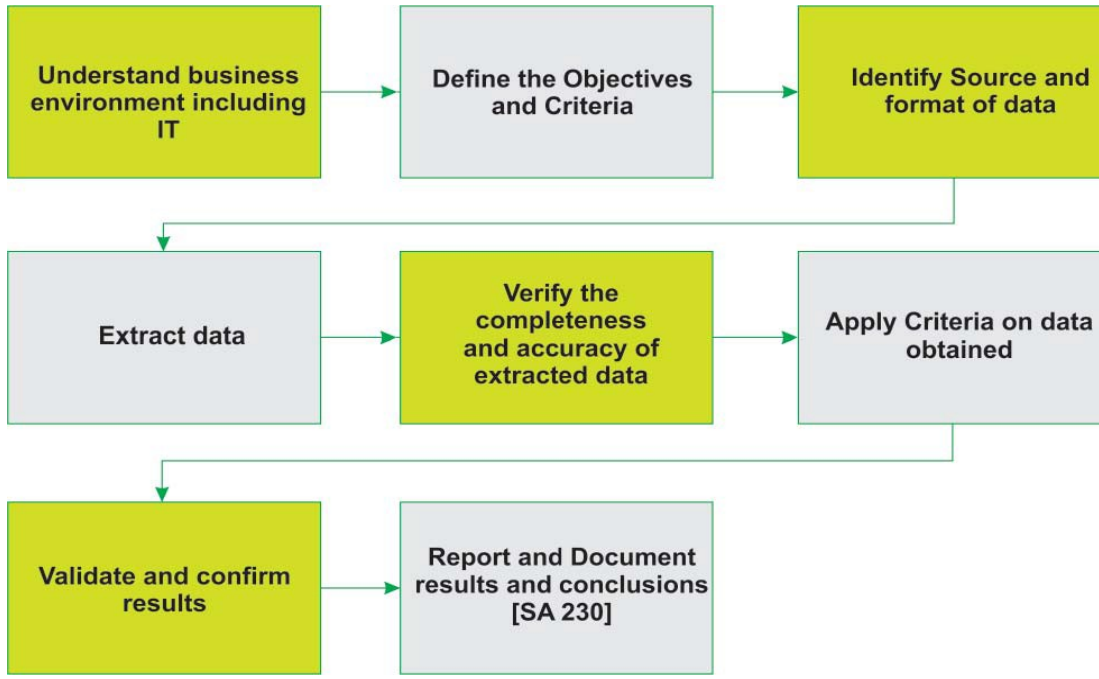
The combination of processes, tools and techniques that are used to tap vast amounts of electronic data to obtain meaningful information is called data analytics. While it is true that companies can benefit immensely from the use of data analytics in terms of increased profitability, better customer service, gaining competitive advantage, more efficient operations, etc., even auditors can make use of similar tools and techniques in the audit process and obtain good results. The tools and techniques that auditors use in applying the principles of data analytics are known as Computer Assisted Auditing Techniques or CAATs in short.

Data analytics can be used in testing of electronic records and data residing in IT systems using spreadsheets and specialised audit tools viz., IDEA and ACL to perform the following:

- Check completeness of data and population that is used in either test of controls or substantive audit tests.
- Selection of audit samples – random sampling, systematic sampling.
- Re-computation of balances – reconstruction of trial balance from transaction data.
- Reperformance of mathematical calculations – depreciation, bank interest calculation.
- Analysis of journal entries as required by SA 240.
- Fraud investigation.
- Evaluating impact of control deficiencies.

There are several steps that should be followed to achieve success with CAATs and any of the supporting tools.

A suggested approach to benefit from the use of CAATs is given in the illustration below:



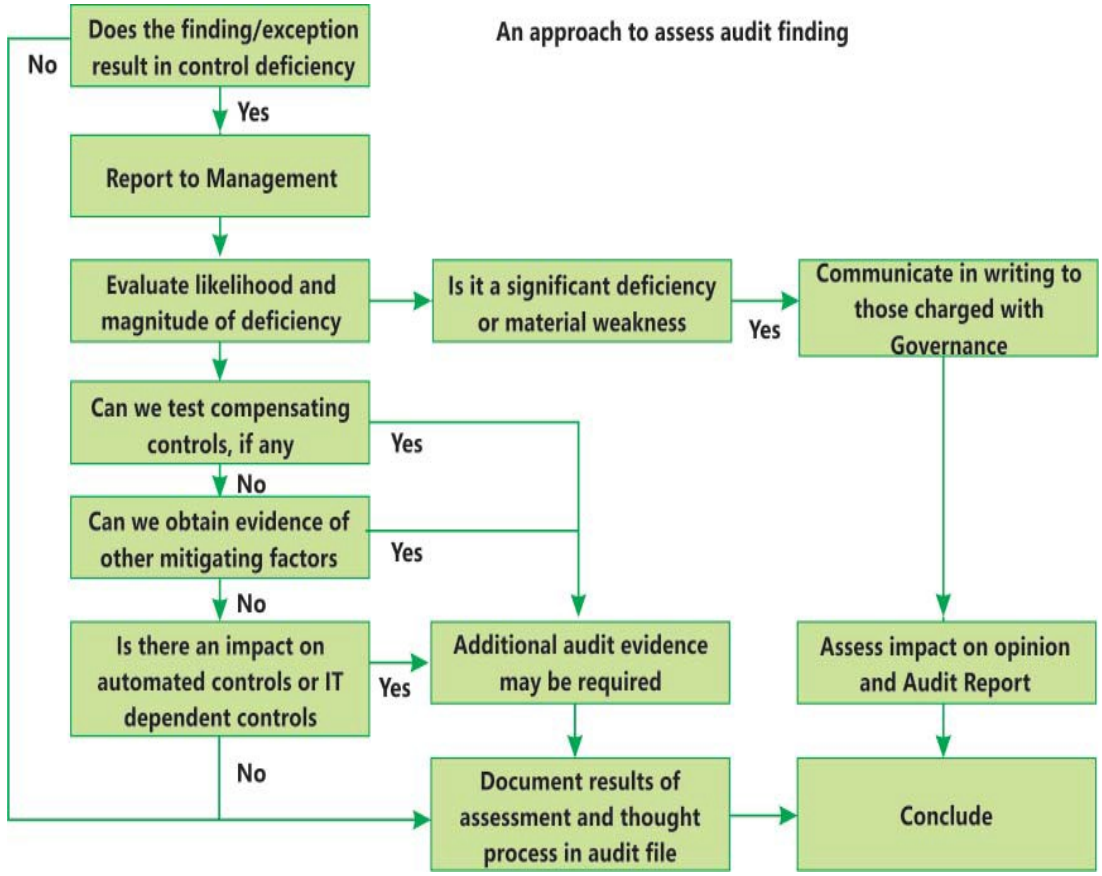
7. ASSESS AND REPORT AUDIT FINDINGS

At the conclusion of each audit, it is possible that there will be certain findings or exceptions in IT environment and IT controls of the company that need to be assessed and reported to relevant stakeholders including management and those charged with governance viz., Board of directors, Audit committee [Students may refer SA 260 (Revised) – *Communication with Those Charged with Governance for more details*].

Some points to consider are as follows:

- Are there any weaknesses in IT controls?
- What is the impact of these weaknesses on overall audit?
- Report deficiencies to management – Internal Controls Memo or Management Letter.
- Communicate in writing any significant deficiencies to Those Charged With Governance.

The auditor needs to assess each finding or exception to determine impact on the audit and evaluate if the exception results in a deficiency in internal control. Refer to the flowchart to learn how this assessment should be carried out. This approach and thought process is the same when auditing in an automated environment or when auditing in a more manual environment.



A deficiency in internal control exits if a control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or the control is missing.

Evaluation and assessment of audit findings and control deficiencies involves applying professional judgement that include considerations for quantitative and qualitative measures. Each finding should be looked at individually and in the aggregate by combining with other findings/deficiencies.

The illustration below is an example of a control deficiency in General IT Controls and how this audit finding is reported to management.

7.1 Reporting Audit Findings – An Illustration

Password resets should be supported with proper request.	
Observation	As per Information Security Policy User A]ccess changes should be initiated and approved. However, we observed that there is no formal process being followed for password reset in SAP. Password reset requests are presently communicated over phone and there is no supporting documentation being maintained for password reset requests. [Ref Information Security policy sub-section no.....]
Exposure	Passwords of User ID with critical privileges may be reset and misused. Non-compliance with Information Security Policy.
Recommendations	It is recommended that all password resets should be requested through a formal process. Adequate supporting documentation should be maintained for user changes in SAP, including password resets, and reviewed periodically.
Management Response	Comments

GLOSSARY

Applications	These are computer software programs that provide a medium for recording, storage and retrieval of business operations or transactions in electronic format.
Audit evidence	This is the data, information, reports that an auditor obtains during audit and forms the basis for an audit opinion.
Automated	A task or activity that is routinely performed by a computer system and does not require manual effort.
CAATs	Short form for Computer Assisted Audit Techniques, are a collection of computer based tools and techniques that are used in an audit for analysing data in electronic form to obtain audit evidence.

Control Deficiency	Exists when an internal control is either missing or not operating effectively to prevent or detect a misstatement in a timely manner by management.
Data	Refers to the digital content that is stored in electronic form within computer systems.
Data Analytics	A combination of processes, tools and techniques that are used to tap vast amounts of electronic data to obtain meaningful information.
Data Processing	Refers to the systematic recording, storage, retrieval, modification and transformation of electronic data using information systems.
Database	A logical subsystem within a larger information system where electronic data is stored in a predefined form and retrieved for use.
Direct Data Change	A backend modification that is made directly to data that is stored in a database bypassing business rules built-in to a business application software.
ERP Enterprise Resource Planning	A type of business application software that provides an integrated platform to automate multiple interrelated business processes and operations.
Financial Reporting	Refers to the process of preparation, presentation and disclosure of financial statements in accordance with a specified reporting framework.
General (IT) Controls	Are a type of internal controls that help in mitigating risks that arise due to use of information technology and information systems in a business.
Information	Electronic data residing in computer systems that is organised in a logical and meaningful manner that is easy to read, understand and analyse.
Information Systems	Refers to a collection of electronic hardware, software, networks and processes that are used in a business to carry out operations and transactions.
Information Technology	The branch of science and engineering that involves designing, building, implementing and maintaining computer systems and networks that can be used in a

	variety of ways including operating businesses and setting up information systems.
Internal Controls	Are the policies and procedures that a company implements to ensure efficiency of business operations, reliability of financial reporting, compliance with laws & regulations, safeguarding of assets and prevention of frauds.
Mainframe	A term that is used to describe a very large computer with high computing power, memory and storage that are required for running large business operations. In addition to business operations, Mainframes are also used in fields of Research & Development, Space, Healthcare, Weather, etc.
Material Weakness	A control deficiency or a combination of deficiencies in internal controls that is important enough to merit the attention of those charged with governance since there is a reasonable possibility that a material misstatement will not be prevented or detected in a timely manner by management.
Operating System	Refers to a system software that is installed in a computer to convert high level user instructions or commands into low level machine understandable format and enable interaction with a computer.
Privileged access	A type of super user access to information systems that enforces less or no limits on using that system.
Risk	A possibility of something that can go wrong in a business process, transaction or operation and could result in a loss.
Segregation of duties	A type of internal control that is implemented in a company to prevent two or more conflicting functions from being assigned to or being carried out by the same person.
Significant Deficiency	A control deficiency or a combination of deficiencies in internal controls that is important enough to merit the attention of those charged with governance since there is a reasonable possibility that a misstatement will not be prevented or detected in a timely manner by management.
Software	A computer program or a collection of computer programs

	that provides an interface to a user for performing a specific activity, task, operation or transaction in electronic form through a computer or information system.
System	Refers to a collection of electronic hardware, software, networks and processes that are used in a business to carry out operations and transactions.

ABBREVIATION

IS	Information System
ATM	Automated Teller Machine
SA	Standards on Auditing
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ELC	Entity Level Controls
FSLI	Financial Statement Line Item
GITC	General Information Technology Controls
IPE	Information Produced by Entity
FSA	Financial Statement Assertion
RCM	Risk & Control Matrix
NTE	Nature, Timing & Extent
ICM	Internal Controls Memorandum
SOD	Segregation of Duties
ERM	Enterprise Risk Management
COSO	Committee of Sponsoring Organisations
CAATS	Computer Assisted Auditing Techniques
ACL	Audit Command Language (CAAT Tool)
ISO	International Organization for Standardization
IFC	Internal Financial Controls

IFC-FR	Internal Financial Controls over Financial Reporting
ICFR	Internal Controls over Financial Reporting
SOX	Sarbanes Oxley Act of 2002
PCI - DSS	Payment Card Industry - Data Security Standard
ITIL	Information Technology Infrastructure Library
COBIT	Control Objectives for Information and Related Technologies
SOC	Service Organisation Controls
SSAE	Statement on Standards for Attest Engagements
ISAE	International Standards for Assurance Engagements
UAT	User Acceptance Testing
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
DBA	Data Base Administrator
Sysadmin	Systems Administrator

SUMMARY

An automated environment basically refers to a business environment where the processes, operations, accounting and even decisions are carried out by using computer systems – also known as Information Systems (IS) or Information Technology (IT) systems.

The fundamental principle of an automated environment is the ability carry out business with less manual intervention and more system driven. The complexity of a business environment depends on the level of automation.As the complexity, automation and dependence of business operations on IT systems increases, the severity and impact of IT risks too increases accordingly.

The auditor should apply professional judgement in determining and assessing such risks and plan the audit response appropriately. To mitigate the above (and more) risks and maintain the confidentiality, integrity, availability and security of data, companies implement IT controls.

Three types of controls in automated environment are (i)General IT Controls (ii)

Application Controls and (iii) IT-Dependent Controls.

There are basically four types of audit tests that should be used. They are inquiry, observation, inspection and reperformance. Data analytics can be used in testing of electronic records and data residing in IT systems using spreadsheets and specialised audit tools.

A deficiency in internal control exits if a control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or the control is missing. Evaluation and assessment of audit findings and control deficiencies involves applying professional judgement that include considerations for quantitative and qualitative measures.

TEST YOUR KNOWLEDGE

MCQs

1. Which of the following is a General IT control?
   (a) IT Environment
   (b) Application Control
   (c) Access Security
   (d) IT Dependent Control
2. Which of the following is an automated control?
   (a) Program change
   (b) System generated report
   (c) Application control
   (d) Configurations
3. Who is mainly responsible for implementation of internal financial controls in a company?
   (a) Auditors
   (b) Directors
   (c) Employees
   (d) Regulators

4. The Guidance Note on Audit of Internal Financial Controls over Financial Reporting has been issued by?

   (a) ICAI

   (b) SEBI

   (c) MCA

   (d) RBI

5. The standard that requires auditors to analyse journal entries in an audit is?

   (a) SA 260

   (b) SA 230

   (c) SA 315

   (d) SA 240

Correct/Incorrect

State with reasons (in short) whether the following statement is correct or incorrect:

(i) All automated environments are complex.

(ii) In an audit of financial statements, the auditor should plan response to all IT risks.

(iii) General IT controls support the functioning of Application controls.

(iv) Inquiry is often the most efficient audit testing method, but least effective.

(v) Specialised audit tools like IDEA, ACL are required to perform data analytics.

Theoretical Questions

1. Briefly mention three reasons why IT should be considered relevant to an audit of financial statements.

2. Describe how risks in IT systems, if not mitigated, could have an impact on audit

3. What are the different testing methods used when auditing in an automated environment. Which is the most effective and efficient method of testing?

ANSWERS/SOLUTIONS

Answers to MCQs

1. (c) **2.** (d) **3.** (b) **4.** (a) **5.** (d)

Answers to Correct/Incorrect

(i) **Incorrect**: The complexity of an automated environment depends on various factors including the nature of business, level of automation, volume of transactions, use of ERP and so on. There could be environment where dependence on IT and automation is relatively less or minimal and hence, considered less complex or even non-complex.

(ii) **Incorrect.** The auditor should plan response to those IT risks that are relevant to financial reporting and not "all" IT risks.

(iii) **Correct.** General IT controls support the functioning of automated application controls and IT dependent controls.

(iv) **Correct.** Inquiry is the most efficient but least effective. Moreover, testing through inquiry alone is not sufficient. Inquiry should be corroborated by applying any one or a combination of observation, inspection or reperformance.

(v) **Incorrect.** Even though specialised audit tools are very useful, such tools are not always required or necessary to carry out data analytics. More commonly available spreadsheet applications like MS-Excel can also be effectively used for carrying out data analytics.

Answers to Theoretical Questions

1. The auditor should consider relevance of IT in an audit of financial statements for the following reasons:

   (a) Since auditors rely on the reports and information generated by IT systems, there could be risk in the IT systems that could have an impact on audit.

   (b) Standards on auditing SA 315 and SA 330 require auditors to understand, assess and respond to risks that arise from the use of IT systems.

   (c) By relying on automated controls and using data analytics in an audit, it is possible to increase the effectiveness and efficiency of the audit process.

2. When risks in IT systems are not mitigated the audit impact could be as follows:

   (i) The auditor may not be able rely on the reports, data obtained, automated controls, calculations and accounting procedures in the IT system.

   (ii) The auditor has to perform additional audit work by spending more time and efforts.

   (iii) The auditor may have to issue a modified opinion, if necessary.

3. When auditing in an automated environment, the following testing methods are used:

   (a) Inquiry

   (b) Observation

   (c) Inspection

   (d) Reperformance

   A combination of inquiry and inspection is generally the most effective and efficient testing method. However, determining the most effective and efficient testing method is a matter of professional judgement and depends on the several factors including risk assessment, control environment, desired level of evidence required, history of errors /misstatements, complexity of business, assertions being addressed.