CHAPTER 4

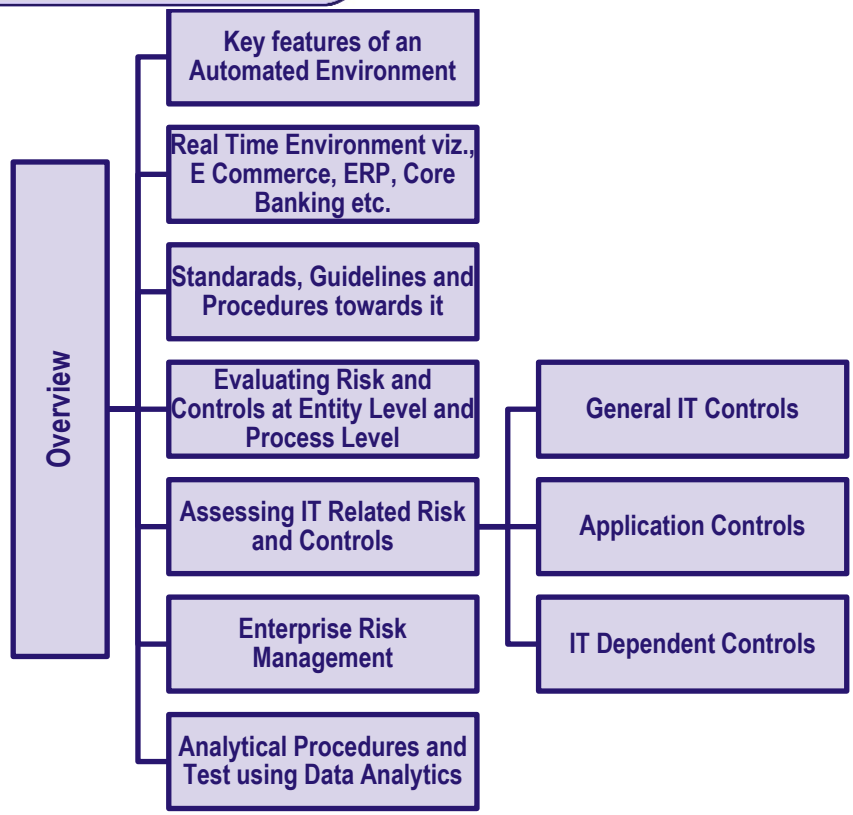
SPECIAL ASPECTS OF AUDITING IN AN AUTOMATED ENVIRONMENT

LEARNING OUTCOMES

After studying this chapter, you will be able to:

- Understand the key features of an automated environment and key concepts of auditing in real-time automated environment such as e-commerce, ERP, core banking.
- Learn how to document the understanding of an automated environment.
- Know how to perform an evaluation of risks and controls at entity level and process level.
- Gain the knowledge of how to assess IT-related risks and controls that exist in an automated environment.
- Gain an overview of enterprise risk management.
- Learn about relevant analytical procedures and tests using data analytics.
- Understand the available standards, guidelines and procedures, frameworks and best practices that are relevant to an automated environment.
- Know the considerations of automated environment at each phase of audit cycle.

CHAPTER OVERVIEW



1. KEY FEATURES OF AN AUTOMATED ENVIRONMENT

An automated environment is an ecosystem that combines people, processes and technology within an overall business environment. Typically, the automated environment is driven by computer based systems which are also known as information technology (IT) systems or information systems (IS). There are several types of applications that could exist in a business depending on several factors including the nature, size, location of a business. Business applications can be broadly categorised as follows:

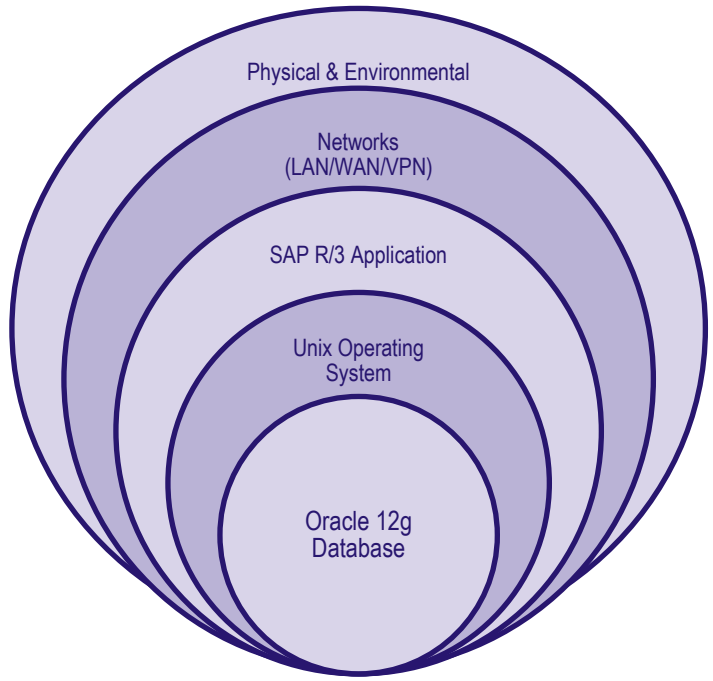
Category of Business Applications	Example of Category
Packaged software (also called off-the-shelf applications) used by micro and small business.	For example, Tally, QuickBooks.

Small ERPs used in small to medium business.	For example, Tally ERP, SAP Business One, Focus ERP.
ERP applications used in medium to large companies.	For example, SAP R/3, Oracle R12 Enterprise Business Suite.

The applications described above form one layer of the overall automated environment. The other layers are made up of the technology infrastructure and the physical & environmental aspect including:

- Databases - Oracle 12g, MS-SQL Server;
- Operating systems - Windows, Unix, Linux;
- Storage devices - disks, tapes, network storage;
- Network devices - switches, routers and firewalls;
- Networks - local area networks, wide area networks, virtual private networks, etc.;
- Physical and environmental – access to IT facilities, CCTVs, temperature control, firefighting equipment, etc.

The illustration below shows the various layers of an automated environment:



It is also likely that some automated environments could have more than one application being used.

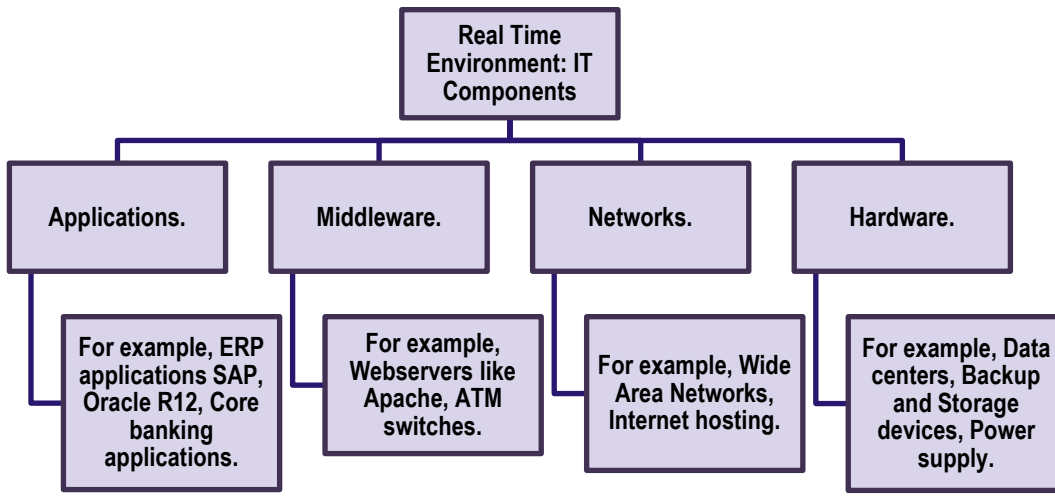
In a hotel there could be one application for front desk & reservations, another application for restaurant & kitchen orders, a guest billing system, and an accounting system. In large multinational companies, specifically in the financial services, the number of applications could be hundreds and even thousands of applications.

2. KEY CONCEPTS OF AUDITING IN REAL-TIME ENVIRONMENT SUCH AS E-COMMERCE, ERP, CORE BANKING, ETC.

A real-time environment is a type of automated environment in which business operations and transactions are initiated, processed and recorded immediately as they happen without delay.

In a bank that is using core banking system a customer account balance is instantly updated when the customer withdraws cash from an ATM. If there is a time delay in updating the customer account, there is a risk that the customer may initiate another transaction through internet or mobile banking channel and this could result in withdrawing more than account balance. Similarly, when a customer makes an online order on a shopping e-commerce portal using credit card, the credit limit of the customer will be reduced immediately.

A real-time environment has several critical IT components that enable anytime, anywhere transactions to take place. They include:



To facilitate transactions in real-time, it is essential to have the systems, networks and applications available during all times. Any failure even in one component could render the real-time system unavailable and could result in a loss of revenue.

If an e-commerce portal that normally processes a several hundred of orders per day goes down for an hour due to a malware attack on one of the webservers hosting the portal, the revenue loss could be significant.

Most real-time systems and environments are accessible through public domain and internet and hence, they are more likely to be vulnerable to network and cyber-attacks including denial of service, distributed denial of service.

Hence, it is critical for a company that operates in a real-time environment to constantly monitor all the IT components to identify and resolve issues and failures. Understanding of the automated environment, the risks and controls that should be considered and audit approach will be covered in the following sections of this chapter.

3. UNDERSTANDING AND DOCUMENTING AUTOMATED ENVIRONMENT

Understanding of the automated environment of a company is required as per SA 315. The auditor's understanding of the automated environment should include the following:

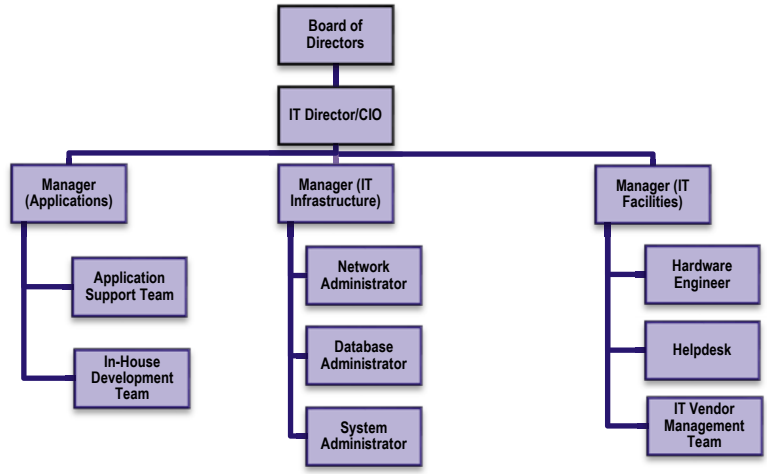
- The applications that are being used by the company;
- Details of the IT infrastructure components for each of the application;
- The organisation structure and governance;
- The policies, procedures and processes followed;
- IT risks and controls.

The auditor is required to document the understanding of a company's automated environment as per SA 230.

The illustration below is an example of how an auditor can document details of an automated environment:

Application	Used for	Database	Operating System	Network	Storage
SAP R/3	Financial Accounting	Oracle 12g	HP-UX	LAN, WAN	NAS
REVS	Front Desk, Guest Reservations	MS-SQL Server 2008	Windows 2012 Server	In-house developed	Server Internal HDD
KOTS	Restaurant and Kitchen Orders	MS-SQL Server 2008	Windows 2012 Server	In-house developed	Server Internal HDD
BILLSYS	Billing	Oracle 11i	Windows 2008 Server	Packaged Software	Server Internal HDD

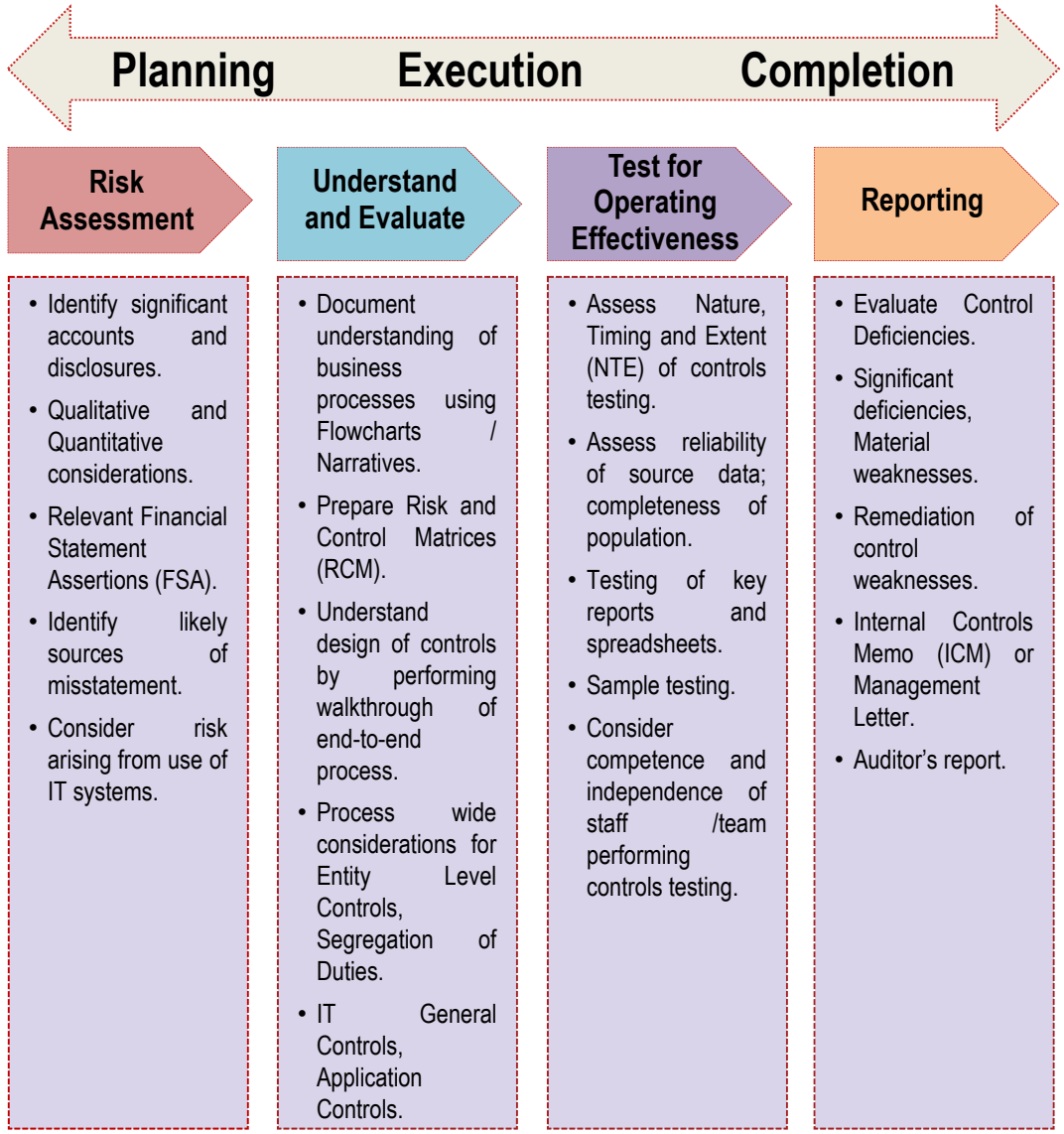
The illustration below is an example of an IT organization:



4. CONSIDERATION OF AUTOMATED ENVIRONMENT AT EACH PHASE OF AUDIT CYCLE

In a controls-based audit, the audit approach can be classified into three broad phases comprising of planning, execution, and completion. In this approach, the considerations of automated environment will be relevant at every phase as given below:

- during risk assessment, the auditor should consider risk arising from the use of IT systems at the company;
- when obtaining an understanding of the business process and performing walkthroughs the use of IT systems and applications should be considered;
- while assessing the entity level controls the aspects related to IT governance need to be understood and reviewed;
- pervasive controls including segregation of duties, general IT controls and applications should be considered and reviewed;
- during testing phase, the results of general IT controls would impact the nature, timing and extent of testing;
- when testing of reports and information produced by the entity (IPE) generated through IT systems and applications;
- at completion stage, evaluation of control deficiencies may require using data analytics and CAATs.



5. ENTERPRISE RISK MANAGEMENT OVERVIEW

Businesses today operate in a dynamic environment. The volatility, unpredictability and pace of changes that exist in the business environment today is far greater than in the past. Some of the reasons for this dynamic environment include globalisation, use of technology, new regulatory requirements, etc. Because of this dynamic environment the associated risks to business have also increased and companies have a need to continuously manage risks.

Examples of risks include:

- Market Risks;
- Regulatory & Compliance Risks;
- Technology & Security Risks;
- Financial Reporting Risks;
- Operational Risks;
- Credit Risk;
- Business Partner Risk;
- Product or Project Risk;
- Environmental Risks.

Risk is the possibility that something could go wrong. In other words, Risk is the possibility that an event will happen which prevents a company from achieving business objectives. Risk Management is a combination of process, people, tools and techniques through which companies identify, assess, respond, mitigate and monitor risks. Enterprise Risk Management is a formal program or framework that is implemented across an enterprise or company for enabling risk management.

Globally, companies in several countries are required by law to have a formal enterprise risk management program. In India, the Companies Act, 2013 requires the board report to include a statement indicating development and implementation of a risk management policy for the company including identification therein of elements of risk, if any, which in the opinion of the board may threaten the existence of the company. The existence of an appropriate system of internal financial control does not by itself provide an assurance to the board of directors that the company has developed and implemented an appropriate risk management policy. While the law makes the Board of directors responsible, an Enterprise Risk Management program of a company is implemented by the board of directors, top management and employees across all levels.

The internal control framework of a company is not separate, though it is an integral part of an Enterprise Risk Management program. The scope of an Enterprise Risk Management program is much broader than an internal control framework and encompasses both internal and external factors that are relevant to business strategy, governance, business process and transaction and activity level. The focus of an internal control framework is primarily around financial reporting, operations and compliance risks associated with an account balance, business process, transaction and activity level, which form a sub-set of the overall enterprise risks.

One of the most common framework that is suitable for implementing an effective enterprise risk management is the COSO Enterprise Risk Management – Integrated Framework developed by the Committee of Sponsoring Organisations (COSO) in 2004 and subsequently updated in 2016 to address the changes in business environment.

One of the most critical component of Enterprise Risk Management is the Risk Assessment process. **The risk assessment process involves considerations for:**

- qualitative and quantitative factors;
- definition of key performance and risk indicators;
- risk appetite;
- risk scores, scales and maps;
- use of data & metrics;
- benchmarking.

A typical risk assessment process would be as given below:

Apart from COSO framework, another relevant and widely available framework is the ISO 31000 Risk Management standard published by the International Organization for Standardization. The ISO 31000:2009, published in 2009, provides a set of principles and guidelines and risk assessment techniques for implementing a risk management framework in a company.

6. ASSESSING IT-RELATED RISKS AND CONTROLS

The auditing standards SA 315 and SA 330 require an auditor to understand, assess and respond to the risks within a company, including those risks that pertain to the use of IT systems and applications in an automated environment. When assessing IT risks in the automated environment, the auditor should consider the following:

- **Entity level aspects of risks that are related to the governance, organisation and management of IT.**

  example

  Has management established an IT Security Policy (Control Environment), communicated the policy to all employees and provided relevant training (Information & Communication)?

  How does management monitor adherence to the established policies (Monitoring)?

- **Risks in the IT processes and procedures being followed.**

  example

  Are unauthorised changes to IT systems applications prevented and detected in a timely manner?

  Is user access to systems commensurate with roles and responsibilities of the user?

- **IT risks at each layer of the automated environment.**

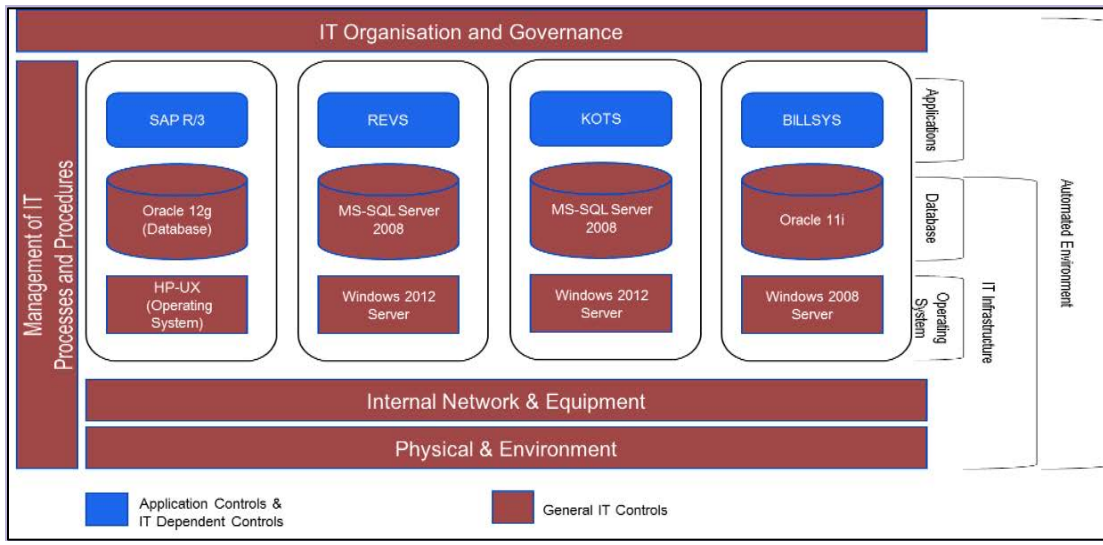
Are direct data changes to database prevented, are strong passwords used in the operating system?

As systems evolve and version updates happen so will new risks emerge. For example, as systems these days are highly interconnected and accessible through public networks like the internet, cyber risks are an emerging threat.

The controls that are put in place to mitigate the IT risks and to maintain the confidentiality, integrity, availability and security of data are as follows:

- General IT Controls;
- Application Controls;
- IT-Dependent Controls.

The illustration below is a sample representation of the various components of an automated environment and where the different types of IT controls fit into the overall environment:



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 environment. 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.

The illustration below is an overview of the Control Objectives and activities for each area of General IT Controls:

Data Center and Network Operations	Program Change	Access Security
Objective: To ensure that production systems are processed to meet financial reporting objectives.	Objective: To ensure that modified systems continue to meet financial reporting objectives.	Objective: To ensure that access to programs and data is authenticated and authorized 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	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	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 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.

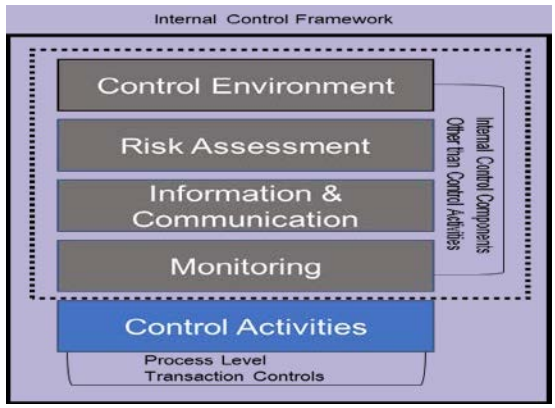
IT dependent controls: IT dependent controls are basically manual controls that make use of some form of data or information or report produced from IT systems and applications. In this case, even though the control is performed manually, the design and effectiveness of such controls depend on the reliability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

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.

7. EVALUATING RISKS AND CONTROLS AT ENTITY LEVEL AND PROCESS LEVEL



Entity Level Risks and Controls: The controls that operate across a company at all levels i.e., from board and top management to the department and transaction level are known as entity level controls or ELCs. **The characteristics of ELCs include the following:**

- Entity Level controls are known as pervasive controls since they operate across all organisation levels.
- ELCs are part of a company's overall internal control framework and relate to the internal control components other than control activities.
- Entity level controls are subjective by nature and hence require application of more professional judgement in their evaluation and testing.

There are direct entity level controls and indirect entity level controls.

(i) **Direct ELCs** operate at a level higher than business activity or transaction level such as a business process or sub-process level, account balance level, at a sufficient level of precision, to prevent, detect or correct a misstatement in a timely manner.

Examples include:

- Business performance reviews;
- Monitoring of effectiveness of controls activities by Internal Audit function;

(ii) **Indirect ELCs** do not relate to any specific business process, transaction or account balance and hence, cannot prevent or detect misstatements. However, they contribute indirectly to the effective operation of direct ELC and other control activities.

Examples include:

- Company code of conduct and ethics policies;
- Human resource policies;
- Employee job roles & responsibilities.

As per these examples, a company that has established policies and procedures, hires people with good background, promotes a culture of fairness and follows ethical practices, is less likely to see the occurrence of a fraud being committed in the company.

From the perspective of an ERP environment, the internal control component that is more relevant is the Information & Communication component.

As part of understanding and evaluation of the Information & Communication component the auditor is required to obtain an understanding of:

- how business processes operate;
- the relevant information systems used in the processing of business transactions and activities;
- the risks and controls pertaining to the information systems and underlying infrastructure;
- reliability of information generated from systems.

While Information & Communication is more relevant to the use of information systems in a company, in large and complex ERP environments it is very likely that the other components of internal controls viz., Control Environment, Risk Assessment and Monitoring will also be relevant.

Auditors are required to understand, evaluate and validate the entity level controls as a part of an audit engagement. The results of testing entity level controls could have an impact on the nature, timing and extent of other audit procedures including testing of controls. **For example**, when the entity level controls at a company are effective, the auditor may consider reducing the number of samples in the test of controls and where the auditor finds the entity level controls ineffective, the auditor may consider to increase the rigour of testing by increasing sample sizes. In small and less complex companies, the entity level controls may not formally defined or documented. In such situations, the auditor should design audit procedures accordingly to obtain evidence of the existence and effectiveness of entity level controls.

The following example shows how the auditor performs an understanding and evaluation of the whistle-blower policy in a company:

- **Does the company have a whistle-blower policy?**
- **Is this policy documented and approved?**
- **Has the whistle-blower policy been communicated to all the employees?**
- **Are employees aware of this policy and understand its purpose and their obligations?**

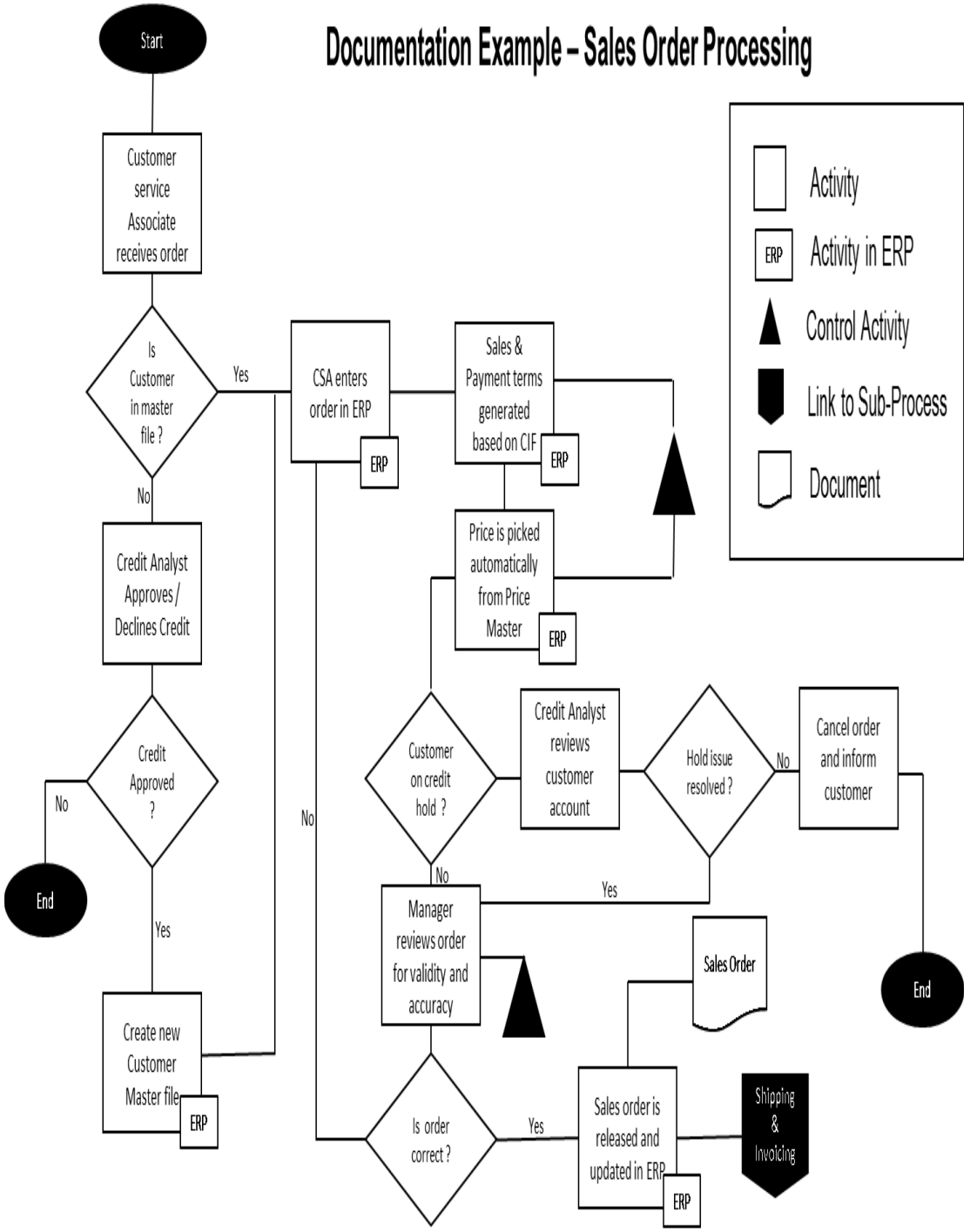
- **Has the company taken measures viz., training, to make the employees understand the contents and purpose of the policy?**
- **Does the company monitor effectiveness of the policy from time-to-time?**
- **How does the company deal with deviations and non-compliance?**

Process Level Risks and Controls: In an audit of financial statements the auditor determines the significant account balances and disclosures. Auditing standards (SA 315) require the auditor to understand the business process that makes up an account balance or financial statement line item (FSLI). A business process is a sequence of activities that take place from the initiation of a transaction, recording it, approving, posting accounting entries and reporting. A business process is typically made up of sub-process - a logical grouping of related activities.

Domestic Sales account balance in the financial statements is an example of an FSLI. The Domestic Sales account balance represents all the sales transactions that were processed during an accounting period. The illustration below shows the business process, sub-process and activities for the Domestic Sales Process - also known as Revenue or OTC (Order to Cash) Process.

Understanding the business process helps the auditor in identification of risks and controls within each process, sub-process and activity. The auditor should document this understanding of the company's business process and flow of transactions in the audit file in accordance with SA 230.

Given below is an example of documentation using flowcharts for one of the sub-process in Domestic Sales process:



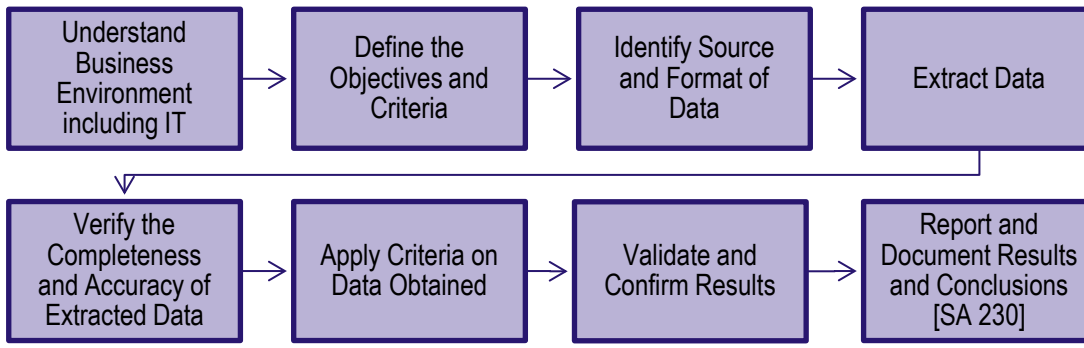
8. USING RELEVANT ANALYTICAL PROCEDURES AND TESTS USING DATA ANALYTICS

In an automated environment, the data stored and processed in systems can be used to get various insights into the way business operates. This data can be useful for preparation of management information system (MIS) reports and electronic dashboards that give a high-level snapshot of business performance. **Generating and preparing meaningful information from raw system data using processes, tools, and techniques is known as Data Analytics.**

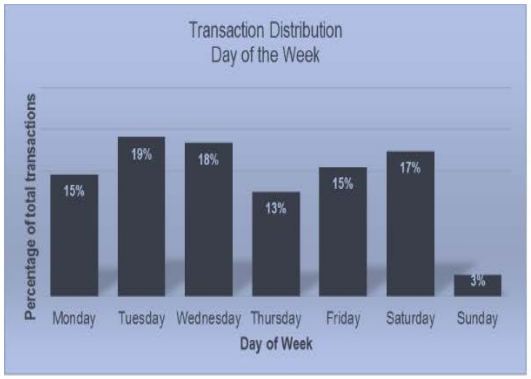
The data analytics methods used in an audit are known as Computer Assisted Auditing Techniques or CAATs. When auditing in an automated environment, auditors can apply the concepts of data analytics for several aspects of an audit including the following:

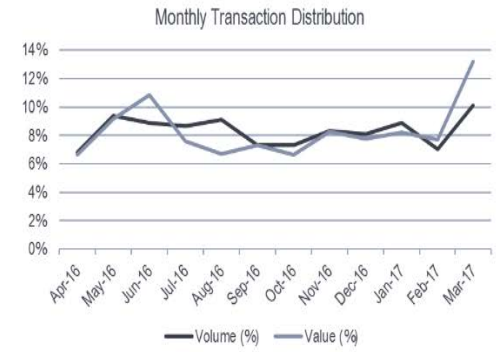
- preliminary analytics;
- risk assessment;
- control testing;
- non-standard journal analysis;
- evaluation of deficiencies;
- fraud risk assessment.

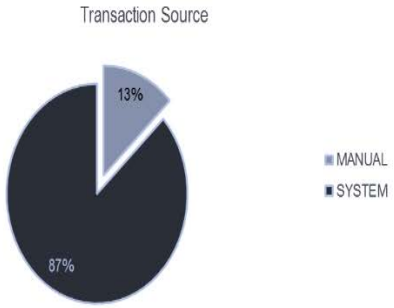
There are several steps that should be followed to achieve success with CAATs and any of the supporting tools. A suggested approach to benefit from the use of CAATs is given in the illustration below:

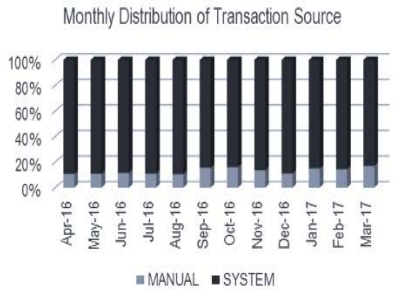


The illustration below is an example of a data analytics dashboard from which an auditor can see a high-level view of the transaction patterns in terms of percentage, volume, distribution and type of transaction. Based on this information the auditor can design appropriate procedures for audit.









9. STANDARDS, GUIDELINES AND PROCEDURES - USING RELEVANT FRAMEWORKS AND BEST PRACTICES

When auditing in an automated environment the auditor should be aware, adhere to and be guided by the various standards, guidelines and procedures that may be relevant to both audit and the automated environment. **Given below are some of the common standards and guidelines that are relevant in this context include:**

- **Standards on Auditing** issued by the Institute of Chartered Accountants of India, are required to be followed for an audit of financial statements.
- **Section 143 of Companies Act 2013** requires statutory auditors to 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. For this purpose, the **Guidance Note on Audit of Internal Financial Controls Over Financial Reporting** issued by the Institute of Chartered Accountants of India, provides the framework, guidelines and procedures for an audit of financial statements.
- **Sarbanes Oxley Act of 2002**, commonly known as SOX, is a requirement in America. Section 404 of this act requires public listed companies to implement, assess and ensure

effectiveness of internal controls over financial reporting and auditors independent opinion on the design and operating effectiveness of internal controls over financial reporting (ICFR) – which is similar to the requirements of IFC-FR for Indian companies. Similar legal and statutory requirements over internal controls exist in several other countries including Japan, China, European Countries, etc.

- **ISO 27001:2013 is the Information Security Management System (ISMS)** standard issued by the International Organization for Standardization (ISO). This standard provides the framework, guidelines and procedures for implementing information security and related controls in a company. For example, this standard covers password security, application security, physical security, backup and recovery, that are relevant when auditing in an automated environment.
- **ITIL (Information Technology Infrastructure Library) and ISO 20000** provide a set of best practice processes and procedures for IT service management in a company. For example, change management, incident management, problem management, IT operations, IT asset management are some of the areas that could be relevant to audit.
- **The Payment Card Industry – Data Security Standard or PCI-DSS**, is the most widely adopted information security standard for the payment cards industry. Any company that is involved in the storage, retrieval, transmission or handling of credit card/debit card information are required to implement the security controls in accordance with this standard.
- The American Institute of Certified Public Accountants has published a **framework under the Statements on Standards for Attest Engagements (SSAE) No.16** for reporting on controls at a service organisation that include
  - **SOC 1 for reporting** on controls at a service organization relevant to user entities' internal control over financial reporting (ICFR).
  - **SOC 2 and SOC 3** for reporting on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy i.e., controls other than ICFR.
  - **While SOC 1 and SOC 2 are restricted use reports, SOC 3 is general use report.**
- **Control Objectives for Information and Related Technologies (CoBIT)** is best practice IT Governance and Management framework published by Information Systems Audit and Control Association. CoBIT provides the required tools, resources and guidelines that are relevant to IT governance, risk, compliance and information security.
- **The Cybersecurity Framework (CSF)** published by the National Institute of Standards and Technology is one of the most popular framework for improving critical infrastructure cybersecurity. This framework provides a set of standards and best practices for companies to manage cybersecurity risks.

GLOSSARY

ERP	**Enterprise Resource Planning**
IT	Information Technology
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-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

TEST YOUR KNOWLEDGE

Theoretical Questions

1. Briefly describe the various stages of a Risk Assessment process.
2. What are the components of an internal control framework?
3. Describe application controls and give three examples of automated application controls.

Multiple Choice Questions

1. KPL Private Limited is a large software company based out of Hyderabad. The annual turnover of the company is INR 2,100 crores. The company sells software and is also involved in the implementation of those softwares for its clients.

   The major chunk of the revenue though comes from sale of software only. The company works on a completely paper-less office and accordingly, most of the documents are available in soft copy.

   During the financial year ended 31 March 2019, the auditors during the course of their audit obtained various audit evidences some of which were in hard copy but mostly in soft copy.

   On conclusion of the audit, the auditors are in a dilemma whether to maintain their documentation entirely in hard copy or soft copy or can it be mixed of both.

   After consultations with various persons, the auditors stood that the documentation for this company, being operated in fully automated environment should be in soft copy only.

   Please advise whether this understanding is correct.

   (a) This is a matter of documentation of audit evidence for a client working in fully automated environment and hence it should be in soft copy only.

   (b) As per the requirements of auditing standards, this documentation can be in a mix of both soft and hard copy.

   (c) Since the client is operating in a fully automated environment, it would be important to check with them because all this documentation has come from the client only.

   (d) As per the requirements of auditing standards, documentation is not required in case of a client working in automated environment because everything is automated and can be accessed easily at any point of time.

2. KJ Private Ltd is engaged in the business of e-commerce wherein most of the operations are automated. The company has SAP at its ERP package and is planning to upgrade the SAP version.

Currently, the version of SAP being used is fine but the higher version would lead to increased efficiencies and hence the company is considering this plan which will also involve a huge outlay.

KPP & Associates, were appointed as the statutory auditors of this company for the year ended 31 March 2019 and the statutory audit firm has been working in this industry for long but most of the work which the firm did was more of risk advisory or internal audit.

For the first time, this audit will be conducted and that's why the audit team started obtaining understanding of the operations of the company which included understanding of the SAP system of the company.

However, the management of the company was not comfortable with this approach of the audit team particularly because audit team was spending good time on understanding of the IT systems of the company.

The management suggested that the auditors should limit their understanding and should perform audit procedures rather than getting into business/ operations.

But the auditors have a different view on this matter and because of which work has got stuck.

In the given situation, please suggest what should be the course of action.

(a) The approach of audit team to obtain detailed understanding of the company before starting with the audit procedures is absolutely fine. If the auditors don't understand the systems properly the audit procedures may not be appropriate.

(b) The management's concern regarding the approach of the auditors seems reasonable. The auditors are spending time on understanding of the systems/ business and not performing their audit procedures.

(c) This being a private company and that too into the business of e-commerce, the auditors should have knowledge about the operations of the company through their understanding of the industry and hence should not get into this process of obtaining detailed understanding at the client place.

(d) The audit team could have planned their work differently. They should involve IT experts who would have knowledge of the systems of the company and hence lot of time can be saved. Further in case of such type of industry, involvement of IT experts is anyways required mandatorily as per the legal requirements.

3. AR Private Limited is a medium-sized company engaged in the business of trading of electronic equipments. The company has various warehouses where all of these equipments are kept and has an inventory levels of generally 2-3 months.

The internal environment of the company is driven by various processes some of them are manual and some automated. Accordingly, the management has also set up various controls both manual and automated and is comfortable with their design and operating effectiveness.

During the course of audit of the financial statements for the year ended 31 March 2019, the auditors raised various queries regarding various processes where the controls were operating effectively. This was because of the fact that auditor was considering either only manual controls or only automated controls in a process.

As per the auditor, the management should have adopted the same approach and hence he would like to increase the substantive audit procedures because they had a view that as per the current approach of the management, controls should be considered as ineffective irrespective of the fact that the testing which the audit team had performed resulted in the controls being effective.

Currently, the concern was regarding the approach on which management was also stuck on their point.

You are required to provide your inputs to resolve this matter.

(a) The approach of the management doesn't seem to be correct because of the nature of the operations of the company. The current approach which the management has followed can be accepted only in case of manufacturing industry.

(b) The management should have discussed their approach with the auditors before appointing them. The Companies Act 2013 provide specific guidance on these matters wherein the management of the company can follow such approach by taking pre-approval from their auditors and in such a case, the report of the auditors is always clean.

(c) The approach of the management is completely fine. The auditors need to correct their understanding of the internal controls and the application of internal controls. A process can not be limited to have either only manual control or automated control.

(d) Considering the size of the company, such matters should be ignored by the auditors. Even if the approach of the management is not correct, it would not have any impact on the work of the auditors because all such matters get resolved at the time when auditors perform final analytical procedures.

4. AJ Private Ltd is in the business of construction and infrastructure having an annual turnover of INR 1,100 crores. The operations of the company are run efficiently driven by the well laid out policies and procedures. The processes of the company are very strong and are well documented and properly communicated to its employees, as required.

The management had also done a detailed risk assessment in the earlier years and currently the risk management system of the company is considered to be very effective. The internal controls include both automated and manual.

During the course of the audit of the financial statements of the company for the financial year ended 31 March 2019, the statutory auditors did their risk assessment and also reviewed the general IT controls which were found to be effective.

Considering the same, one of the senior audit team members asked the team to start performing the substantive audit procedures taking the approach that controls are effective.

However, the audit team did not find this approach correct and discussed that they should also check the effectiveness of other manual and automated controls by testing them and then move on to substantive testing.

The audit team recently had a training on the internal controls and hence their understanding was different from the audit senior.

This led to a conflicting situation between the audit senior and remaining audit team.

In the given situation, please advise which of the following would be correct.

(a) The audit senior is correct because general IT controls were found to be effective and hence no further work may be required on controls.

(b) The view of the audit team looks fine because without testing of internal controls covering all types of controls (manual and automated), those controls can not be said to be operating effectively.

(c) The audit senior seems reasonable in his approach because general IT controls were found to be effective. However, it would be more appropriate to also test application controls before concluding on the effectiveness of the controls.

(d) The argument of the audit team looks better because every audit requires significant time to be spent on testing of internal controls and by only covering general IT controls, it would be difficult to justify this requirement later on in the audit file.

5. RIM Private Ltd is engaged in the business of manufacturing of cranes and other construction equipments. The nature of the operations are such that purchases are quite significant even though the sales may or may not be very significant, in terms of number of transactions during the year.

The company's statutory auditors, have also obtained certain audit tools to help the audit team on various audit procedures to bring efficiency in various audits.

During the course of the audit of the financial statements for the financial year ended 31 March 2019, the auditors used those audit tools (also known as computed assisted audit techniques) for sampling procedures and data analytics.

The outcome of the tools resulted in some analysis and requirements which the audit team requested from the client. However, the client refused to provide any such information

because as per the client all these tools were those of the auditor and any outcome of the same needs to be handled by themselves instead of asking the management.

The auditors have suggested that such an attitude of non-cooperation would not help the either party and would defeat the objective of the audit. The management of the company is, however, ready to provide any other information to the auditors.

In this situation, please advise both the management and the auditors.

(a) Since the management is ready to provide any other information, the auditor should obtain this information as well by not disclosing the management that it is outcome of any audit tool.

(b) The view of the management is correct because audit tools are there to support the auditors and not to lead to increased work for the management.

(c) The auditors are correct because by using audit tools they are performing their audit procedures.

(d) The auditors should ignore all these tools and plan their audit procedures accordingly.

Answers to Theoretical Questions

1. Risk Assessment is one of the most critical components of Enterprise Risk Management. The risk assessment process involves considerations for qualitative and quantitative factors, definition of key performance and risk indicators, risk appetite, risk scores, scales and maps, use of data & metrics and benchmarking. **The various stages in a Risk Assessment process are as follows:**

   - Define Business Objectives and Goals;
   - Identify events that affect achievement of business objectives;
   - Assess likelihood and impact;
   - Respond and mitigate risks;
   - Assess residual risk.

2. There are **five components** of an internal control framework. **They are as follows:**

   - Control Environment;
   - Risk Assessment;
   - Information & Communication;
   - Monitoring;
   - Control Activities.

3. Application Controls are 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.

Answers to Multiple Choice Questions

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