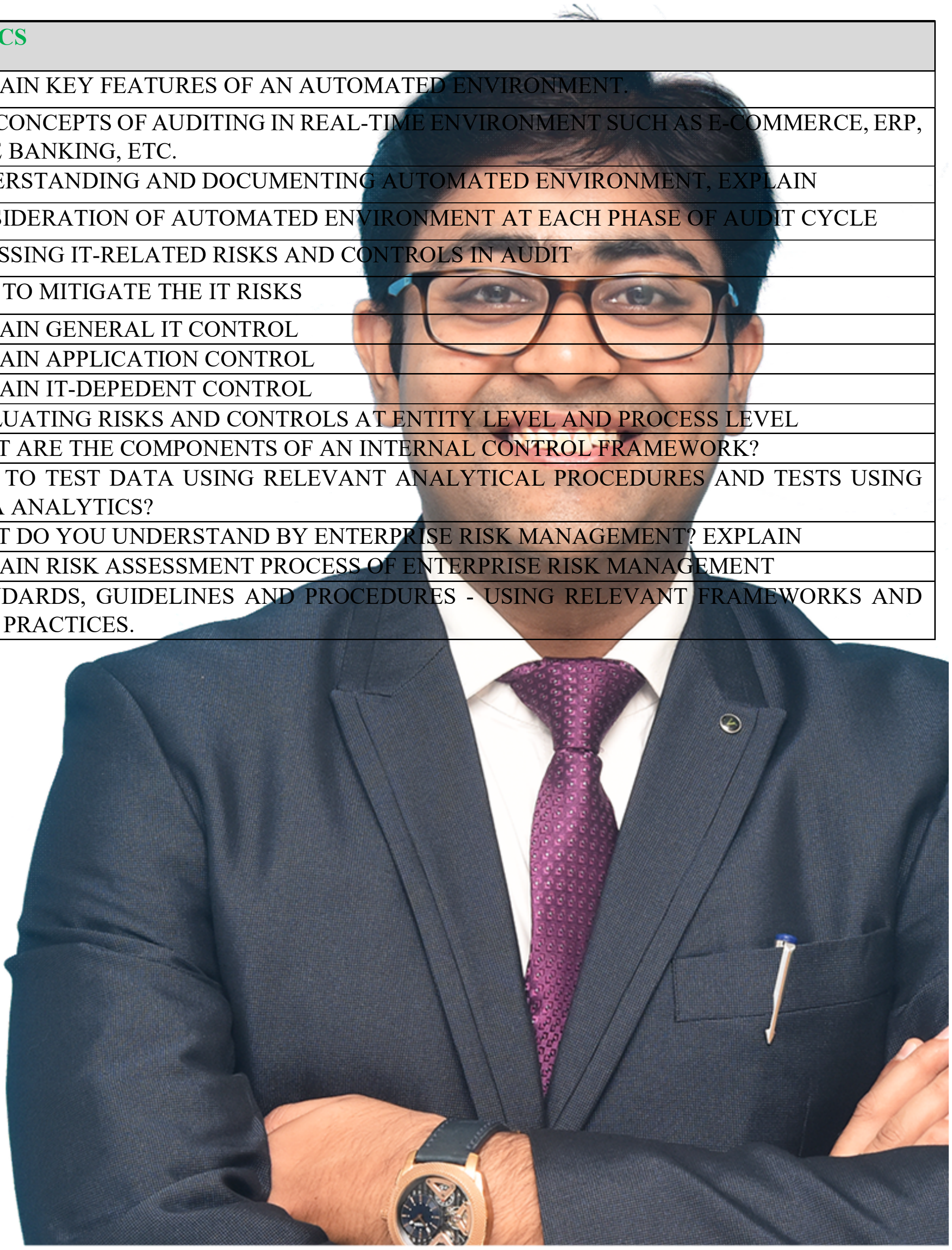
Chapter 4 -

- **AUDITING IN AN AUTOMATED ENVIRONMENTAUDIT OF CONSOLIDATED FINANCIAL STATEMENTS**

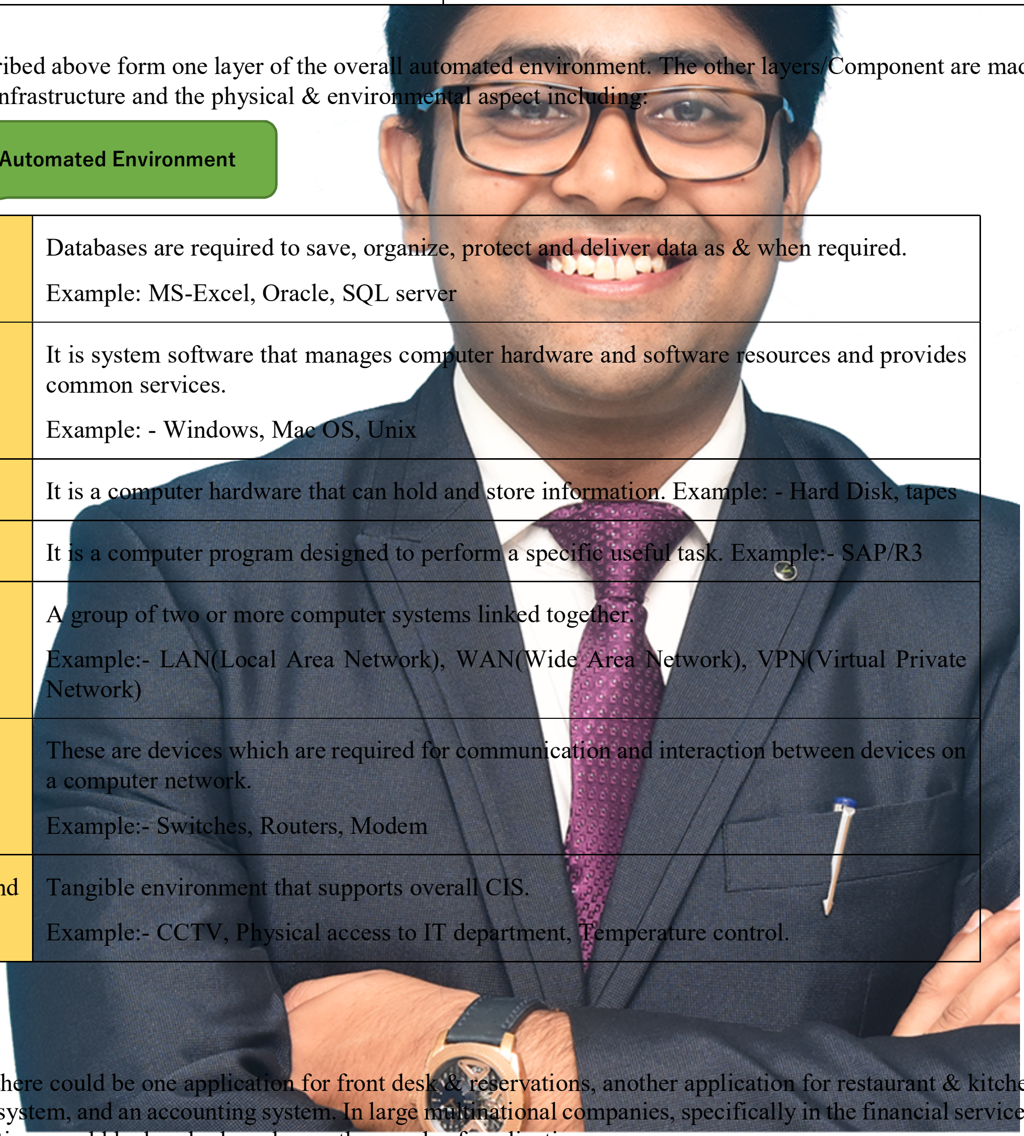
CHAPTER 4	TOPICS
QUS 1	EXPLAIN KEY FEATURES OF AN AUTOMATED ENVIRONMENT.
QUS 2	KEY CONCEPTS OF AUDITING IN REAL-TIME ENVIRONMENT SUCH AS E-COMMERCE, ERP, CORE BANKING, ETC.
QUS 3	UNDERSTANDING AND DOCUMENTING AUTOMATED ENVIRONMENT, EXPLAIN
QUS 4	CONSIDERATION OF AUTOMATED ENVIRONMENT AT EACH PHASE OF AUDIT CYCLE
QUS 5	ASSESSING IT-RELATED RISKS AND CONTROLS IN AUDIT
QUS 6	HOW TO MITIGATE THE IT RISKS
QUS 7	EXPLAIN GENERAL IT CONTROL
QUS 8	EXPLAIN APPLICATION CONTROL
QUS 9	EXPLAIN IT-DEPEDENT CONTROL
QUS 10	EVALUATING RISKS AND CONTROLS AT ENTITY LEVEL AND PROCESS LEVEL
QUS 11	WHAT ARE THE COMPONENTS OF AN INTERNAL CONTROL FRAMEWORK?
QUS 12	HOW TO TEST DATA USING RELEVANT ANALYTICAL PROCEDURES AND TESTS USING DATA ANALYTICS?
QUS 13	WHAT DO YOU UNDERSTAND BY ENTERPRISE RISK MANAGEMENT? EXPLAIN
QUS 14	EXPLAIN RISK ASSESSMENT PROCESS OF ENTERPRISE RISK MANAGEMENT
QUS 15	STANDARDS, GUIDELINES AND PROCEDURES - USING RELEVANT FRAMEWORKS AND BEST PRACTICES.



QUS1 - 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). Business applications can be broadly categorized 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/Component are made up of the technology infrastructure and the physical & environmental aspect including:

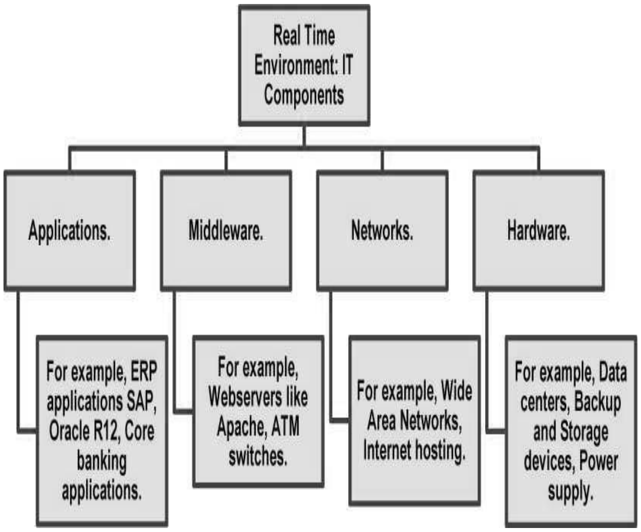
Component of Automated Environment

Databases	Databases are required to save, organize, protect and deliver data as & when required. Example: MS-Excel, Oracle, SQL server
Operating systems	It is system software that manages computer hardware and software resources and provides common services. Example: - Windows, Mac OS, Unix
Storage devices	It is a computer hardware that can hold and store information. Example: - Hard Disk, tapes
Application	It is a computer program designed to perform a specific useful task. Example:- SAP/R3
Network devices	A group of two or more computer systems linked together. Example:- LAN(Local Area Network), WAN(Wide Area Network), VPN(Virtual Private Network)
Networks	These are devices which are required for communication and interaction between devices on a computer network. Example:- Switches, Routers, Modem
Physical and environmental	Tangible environment that supports overall CIS. Example:- CCTV, Physical access to IT department, Temperature control.

Example - 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.

QUS2- EXPLAIN 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. **Example Banking, Railway, Online Shopping.**


Real Time Environment: IT Components
Applications.
Middleware.
Networks.
Hardware.
For example, ERP applications SAP, Oracle R12, Core banking applications.
For example, Webservers like Apache, ATM switches.
For example, Wide Area Networks, Internet hosting.
For example, Data centers, Backup and Storage devices, Power supply.

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

Example- 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.

QUS 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.

QUS 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/Reporting. In this approach, the considerations of automated environment will be relevant at every phase as given below:

RAP

During risk assessment, the auditor should consider risk arising from the use of IT systems at the company;

- Identify significant accounts and disclosures. Qualitative and Quantitative considerations.
- Relevant Financial Statement Assertions (FSA).
- Identify likely sources of misstatement.
- Consider risk arising from use of IT systems.

Walkthrough

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;

- Document understanding of business processes using Flowcharts / Narratives.
- Prepare Risk and Control Matrices (RCM).
- Understand design of controls by performing walkthrough of end-to-end process.
- Process wide considerations for Entity Level Controls, Segregation of Duties.
- IT General Controls, Application Controls.

Testing

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;

- Assess Nature, Timing and Extent (NTE) of controls testing.
- Assess reliability of source data; completeness of population.
- Testing of key reports and spreadsheets.
- Sample testing.

Completion/Reporting Stage-

Evaluation of control deficiencies may require using data analytics and CAATs

- Evaluate Control Deficiencies.
- Significant deficiencies, Material weaknesses.
- Remediation of control weaknesses.
- Internal Controls Memo (ICM) or Management Letter.
- Auditor's report.

QUS 5 - ASSESSING IT-RELATED RISKS AND CONTROLS IN AUDIT

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:

1. **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)?
2. **Risks in the IT processes and procedures being followed.**
    - **Example -** Are unauthorized changes to IT systems applications prevented and detected in a timely manner
3. **IT risks at each layer of the automated environment.**
    - **Example** - 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.

QUS 6 - HOW TO MITIGATE THE IT RISKS.

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.

QUS7- EXPLAIN GENERAL IT CONTROL

General IT controls are policies and procedures that relate to many applications and support the effective functioning of application controls. They apply to mainframe, mainframe, 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.

QUS8- EXPLAIN APPLICATION CONTROL

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.

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.

QUS9- EXPLAIN IT-DEPEDENT CONTROL

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.

QUS10- EVALUATING RISKS AND CONTROLS AT ENTITY LEVEL AND PROCESS LEVEL

Entity Level Risks and Controls	Process 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	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

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.

Entity Level Risks and Controls:

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

- **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.
- **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.

from the **I R P R**. 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.

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.

QUS11- WHAT ARE THE COMPONENTS OF AN INTERNAL CONTROL FRAMEWORK?

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

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

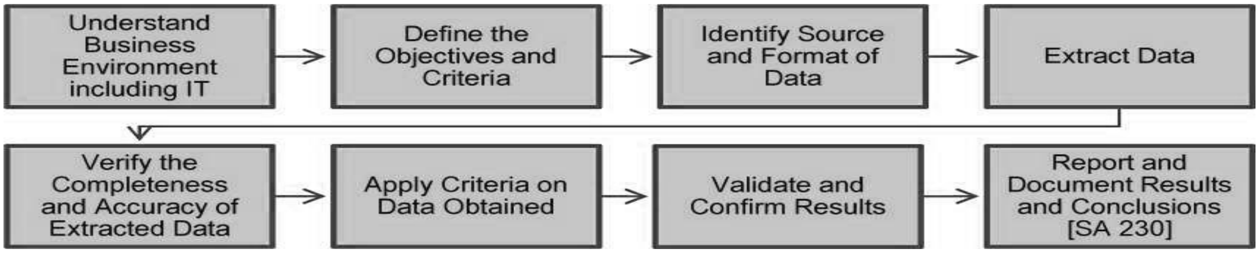
QUS 12- HOW TO TEST DATA USING RELEVANT ANALYTICAL PROCEDURES AND TESTS USING DATA ANALYTICS?

In an automated environment, the data stored and processed in systems can be used to get various insights into the way business operates. **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:



Understand Business Environment including IT → Define the Objectives and Criteria → Identify Source and Format of Data → Extract Data → Verify the Completeness and Accuracy of Extracted Data → Apply Criteria on Data Obtained → Validate and Confirm Results → Report and Document Results and Conclusions [SA 230]

QUS 13- WHAT DO YOU UNDERSTAND BY ENTERPRISE RISK MANAGEMENT? EXPLAIN

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. 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;

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.

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.

One of the most common frameworks 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.

Risk types

The risk and examples include:

1. Hazard risk - Property damage, Natural catastrophe
2. Financial risk - Asset risk, Currency risk, Liquidity risk
3. Operational risk - Customer satisfaction, Product failure, Reputational risk, Internal Poaching, Knowledge drain
4. Strategic risks- Competition, Social trend, Capital availability
5. Regulatory risk
6. Technology risk
7. Environmental risk

Risk response strategy

Management selects a risk response strategy for specific risks identified and analyzed, which may include:

Avoidance - exiting the activities giving rise to risk

Reduction- taking action to reduce the likelihood or impact related to the risk

Alternative Actions- deciding and considering other feasible steps to minimize risks.

Share or Insure - transferring or sharing a portion of the risk, to finance it

Accept - no action is taken, due to a cost/benefit decision

THE INTERNAL CONTROL FRAMEWORK AND ENTERPRISE RISK MANAGEMENT

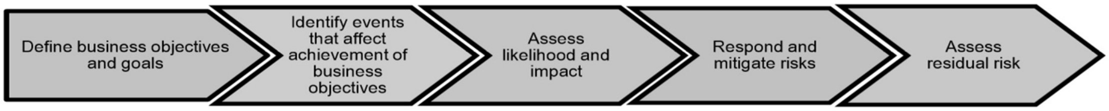
The internal control framework of a company is not separate, though it is an integral part of an Enterprise Risk Management program. The scope of an Enterprise Risk Management program is much broader than an internal control framework and encompasses both internal and external factors that are relevant 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.

QUS 14- EXPLAIN RISK ASSESSMENT PROCESS 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;
- benchmarking.

A typical risk assessment process would be as given below:


Define business objectives and goals
Identify events that affect achievement of business objectives
Assess likelihood and impact
Respond and mitigate risks
Assess residual risk

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.

QUS 15- STANDARDS, GUIDELINES AND PROCEDURES - USING RELEVANT FRAMEWORKS AND BEST PRACTICES.

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.

- **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 frameworks for improving critical infrastructure cybersecurity. This framework provides a set of standards and best practices for companies to manage cybersecurity risks