Date: April 01, 2021

VIRTUAL CLASSES
ORGANISED BY BOS, ICAI

INTERMEDIATE LEVEL
PAPER 7A: ENTERPRISE INFORMATION SYSTEM

Faculty: CA ATUL KUMAR GUPTA, B.COM, FCA, DISA(ICA)

Disclaimer’s and Disclosures

- All trademarks are property of their respective owner’s.
- The presentation is to help students understand the nuances of the subject, get a better grip on it. Any example given is help gain proper perspective to the issue in hand and in no way intended to degrade, denounce any person or and technology being used.
- The presentation is based on study module.
- HAPPY LEARNING…

A request at the start

- Please ask questions during the session’s,
- It adds to learning curve …..
- Thanks

Approach to SUBJECT

- You all have been through many sessions and you realize that subject is absolutely practical….

🙂

SYLLABUS

- Chapter 1: Automated Business Process
- Chapter 2: Financial And Accounting System
- Chapter 3: Information System and Its Components
- Chapter 4: E-Commerce M-Commerce and Emerging Technology
- Chapter 5: Core Banking System

Starting with

- Chapter 1: Automated Business Process

Topics: MAIN

- Introduction
  - Enterprise Business Processes
  - Automated Business Processes
  - Risk and Its Management
  - Enterprises Risk Management
  - Controls
  - Diagrammatic Representation of Business Processes
  - Risks and Controls for Specific Business Processes
  - Regulatory and Compliance Requirements

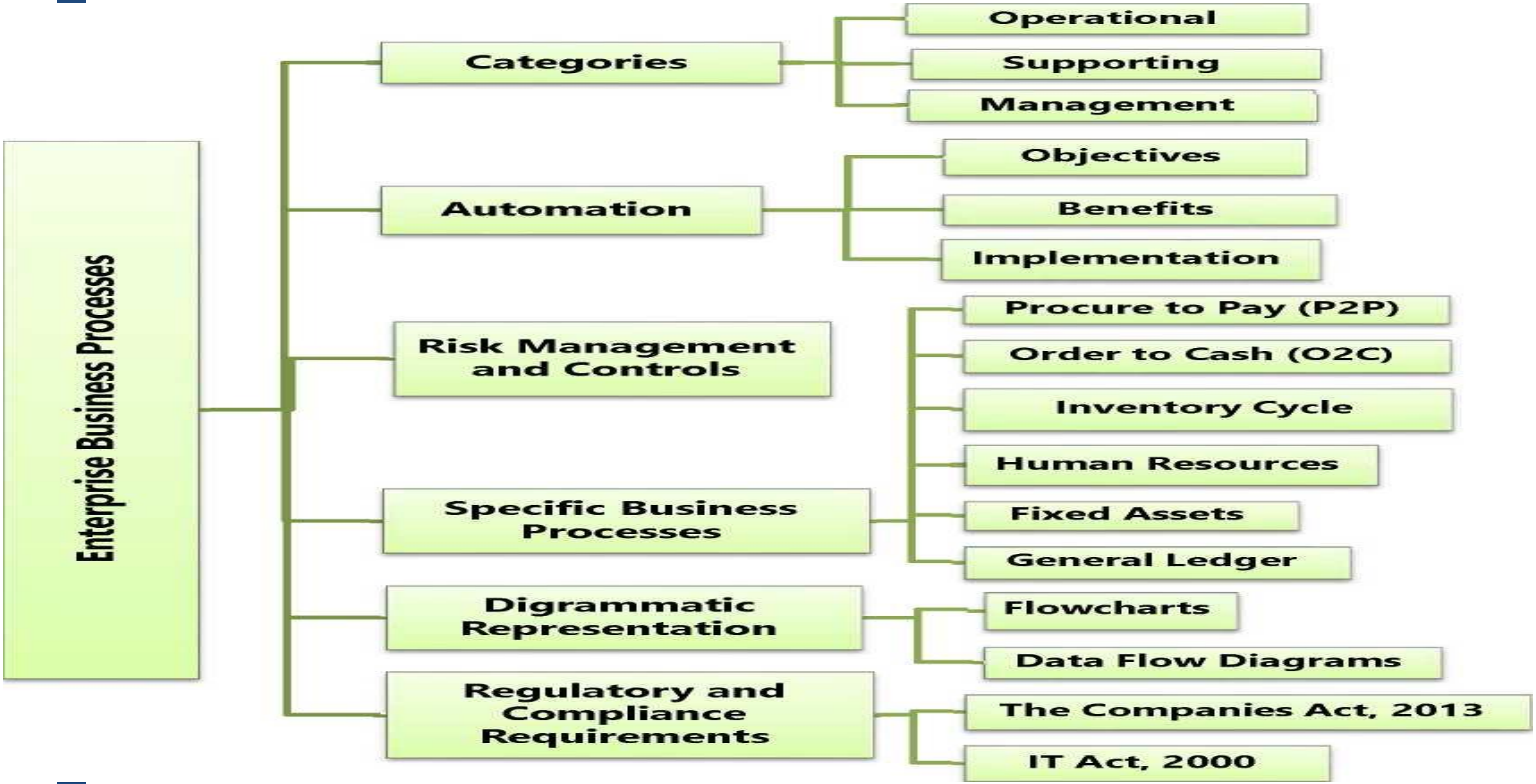
Introduction: CONCEPT

- The concept of integrated and non-integrated system needs good understanding..
- Let us take example:
- Your vehicle suddenly stops as fuel is finished…
- Purchase manager gets an email / sms from the system informing that an important raw material items inventory level has touched re-order level…

Session Plan:

CHAPTER PLAN

- Summary of chapter
- Chapter Content: Mid Chapter MCQs
- Recap of Day


Enterprise Business Processes
Categories
Operational
Supporting
Management
Automation
Objectives
Benefits
Implementation
Risk Management and Controls
Specific Business Processes
Procure to Pay (P2P)
Order to Cash (O2C)
Inventory Cycle
Human Resources
Fixed Assets
General Ledger
Digrammatic Representation
Flowcharts
Data Flow Diagrams
Regulatory and Compliance Requirements
The Companies Act, 2013
IT Act, 2000

Chapter 1: AUTOMATED BUSINESS PROCESS

Learning Objectives

- Build an understanding on the concepts of Business Process, its automation and implementation.
- Understand concepts, flow and relationship of internal and automated controls.
- Acknowledge risks and controls of various business processes.
- Grasp the understanding on the structure and flow of business processes, related risks and controls.
- Comprehend the specific regulatory and compliance requirements of The Companies Act and The Information Technology Act as applicable to Enterprise Information Systems.

Introduction..1

- In today’s connected world where information flows at speed of light, success on any organization depends on its ability to respond to fast changing environment. The capability of any organization depends on its ability to take fast decisions.
- The solution to this problem is provided by Enterprise Information Systems, by collecting data from numerous crucial business processes like manufacturing and production, finance and accounting, sales and marketing, and human resources and storing the data in single central data repository.

Introduction..2

- An **Enterprise Information System (EIS)** may be defined as any kind of information system which improves the functions of an enterprise business processes by integration.
- An EIS provide a technology platform that enables organizations to integrate and coordinate their business processes on a robust foundation.

Topics: MAIN

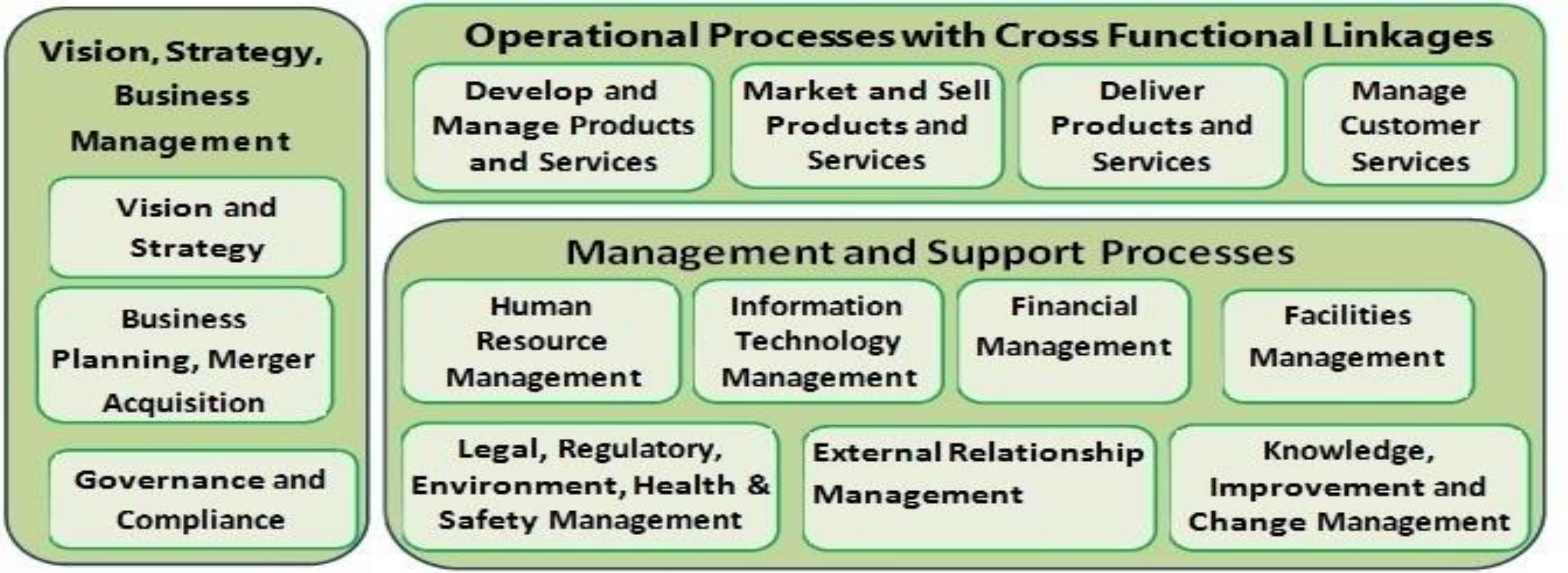
- Introduction
- Enterprise Business Processes
- Automated Business Processes
- Risk and Its Management
- Enterprises Risk Management
- Controls
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

Enterprise Business Process

A **Business Process** is an activity or set of activities that will accomplish a specific organizational goal. Business processes are designed as per vision and mission of top management. Business processes are reflection of entities management thought process. The success or failure of an organization is dependent on how meticulously business processes have been designed and implemented.

Business Process Management (BPM), helps an organization achieve 3E's for business processes, namely **Effectiveness**, **Efficiency** and **Economy**. BPM is a systematic approach to improving these processes. Business Process Management is an all-round activity working on a 24x7 basis to ensure improvement in all parameters all the time.

Enterprise Business Process Model



Vision, Strategy, Business Management

Vision and Strategy

Business Planning, Merger Acquisition

Governance and Compliance

Operational Processes with Cross Functional Linkages

Develop and Manage Products and Services

Market and Sell Products and Services

Deliver Products and Services

Manage Customer Services

Management and Support Processes

Human Resource Management

Information Technology Management

Financial Management

Facilities Management

Legal, Regulatory, Environment, Health & Safety Management

External Relationship Management

Knowledge, Improvement and Change Management

Enterprise Business Categories

Nature of Business Decision	***Description of decision***
Vision and Mission	*One of largest of INDIA conglomerate some two decades ago (Year 20XX) decided to be in those business by 20XX (15 years ahead) in which they can be top 5 companies in the world.*
Management Process	***The Group did all this in next 15 years.*** -Steel company acquisition in UK/EU and Singapore***: Result top 5 steel company in world.*** – The group acquired TEA gardens across the world. – ***Result top sellers of TEA in world.***
Support Process	*For all activities to be done as envisioned by top management, a huge effort was needed on human resources front. This included - Defining and creating a new management structure* - *Performing all human resource activities as listed above.*
Operational Process	*Post the management processes, it is on the operational managers to implement the decisions in actual working form. It is here where the whole hard job is done.*

MCQ 1

ICAI decides that by year 2021 it shall be 100% E-ICAI. This reflects

a. Vision and Mission

b. Management Process

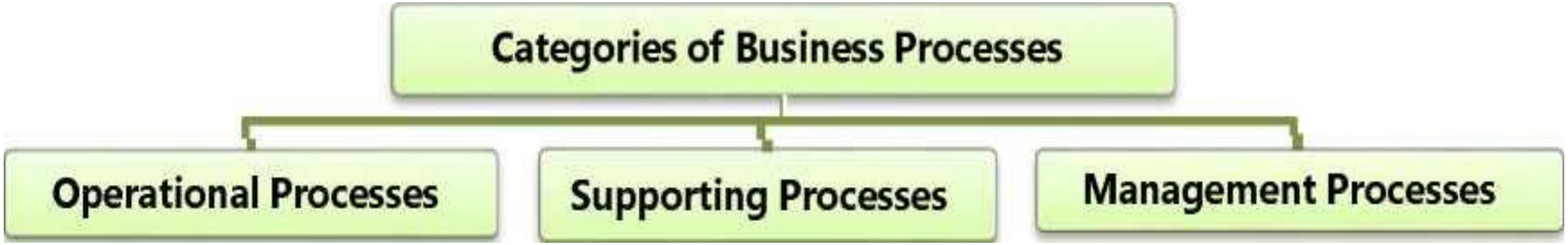
c. Support Process

d. Operational Process

A

Categories of Business Processes

Depending on the organization, industry and nature of work; business processes are often broken up into different categories as shown below.



Categories of Business Processes

Operational Processes

Supporting Processes

Management Processes

Categories of Business Processes

Operational or **Primary Processes** deal with the core business and value chain. These processes deliver value to the customer by helping to produce a product or service. Operational processes represent essential business activities that accomplish business objectives, eg. generating revenue - Order to Cash cycle (O2C), Procurement - Purchase to Pay (P2P) cycle.

Supporting Processes back core processes and functions within an organization. Examples of supporting or management processes include Accounting, Human Resource (HR) Management and workplace safety. One key differentiator between operational and support processes is that support processes do not provide value to customers directly. However, it should be noted that hiring the right people for the right job has a direct impact on the efficiency of the enterprise.

Categories of Business Processes

Management Processes

Management Processes measure, monitor and control activities related to business procedures and systems. Examples of management processes include internal communications, governance, strategic planning, budgeting, and infrastructure or capacity management. Like supporting processes, management processes do not provide value directly to the customers. However, it has a direct impact on the efficiency of the enterprise. **Illustration of budgeting process**

Vision	»	**Strategic Plan**		**Business Goals**	||	**Revenue Projections**		**Cost Projections**	*	**Profit Projections**		**Board Approval**	**Budget Review**

Topics: MAIN

- Introduction
- Enterprise Business Processes
- **Automated Business Processes**
- Risk and Its Management
- Enterprises Risk Management
- Controls
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

Automated Business Process

Today technology innovations are increasing day by day, technology is becoming easily available, cost of accessing and using technology is going down, internet connectivity in term of speed and geographical spread is increasing day by day. All these factors are having a profound impact on the business processes being used by entity.

Factors affecting BPA success

The success of any Business Process Automation shall only be achieved when BPA ensures the following:

- ♦ Confidentiality: To ensure that data is only available to persons who have right to see the same;
- ♦ Integrity: To ensure that no un-authorized amendments can be made in the data;
- ♦ Availability: To ensure that data is available when asked for; and
- ♦ Timeliness: To ensure that data is made available in at the right time.

To ensure that all the above parameters are met, BPA needs to have appropriate internal controls put in place.

MCQ 2

The first aspect PASSWORD will ensure for a BPA is

a. Integrity

b. Confidentiality

c. Timeliness

d. Availability

B

Benefits of Automating Business Process

1) Quality and Consistency

♦ Ensures that every action is performed identically - resulting in high quality, reliable results and stakeholders will consistently experience the same level of service.

2) Time Saving

♦ Automation reduces the number of tasks employees would otherwise need to do manually.

♦ It frees up time to work on items that add genuine value to the business, allowing innovation and increasing employees' levels of motivation.

3) Visibility

♦ Automated processes are controlled and they consistently operate accurately within the defined timeline. It gives visibility of the process status to the organization.

Benefits of Automating Business Process

4) Improved Operational Efficiency

♦ Automation reduces the time it takes to achieve a task, the effort required to undertake it and the cost of completing it successfully.

♦ Automation not only ensures systems run smoothly and efficiently, but that errors are eliminated and that best practices are constantly leveraged.

5) Governance & Reliability

♦ The consistency of automated processes means stakeholders can rely on business processes to operate and offer reliable processes to customers, maintaining a competitive advantage.

Benefits of Automating Business Process

6) Reduced Turnaround Times

♦ Eliminate unnecessary tasks and realign process steps to optimize the flow of information throughout production, service, billing and collection. This adjustment of processes distils operational performance and reduces the turnaround times for both staff and external customers.

7) Reduced Costs

♦ Manual tasks, given that they are performed one-at-a-time and at a slower rate than an automated task, will cost more. Automation allows us to accomplish more by utilizing fewer resources.

BPA: Which Process Should be Automated?

- From Module

BPA: Challenges in BPA

- From Module

BPA Implementation

Step 1: Define why we plan to implement a BPA?

♦ Errors in manual processes leading to higher costs.

♦ Paying for goods and services not received.

♦ Not being able to find documents quickly during an audit or lawsuit or not being able to find all documents

♦ Unable to recruit and train new employees, but where employees are urgently required.

♦ Lack of management understanding of business processes.

BPA Implementation

Step 2: Understand the rules / regulation under which enterprise needs to comply with?

One of the most important steps in automating any business process is to understand the rules of engagement, which include following the rules, adhering to regulations and following document retention requirements. This governance is established by a combination of internal corporate policies, external industry regulations and local, state, and central laws. Entity needs to ensure that any BPA adheres to the requirements of law.

BPA Implementation

Step 3: Document the process, we wish to automate

-What documents need to be captured?

-Where do they come from?

-What format are they in: Paper, FAX, email, PDF etc.?

-Who is involved in processing of the documents

-What is the impact of regulations on processing of these documents?

-Can there be a better way to do the same job?

-How are exceptions in the process handled?

BPA Implementation

Step 4: Define the objectives / goals to be achieved by implementing BPA.

<u>Define the SMART way</u>

- Specific: Clearly defined,
- Measurable: Easily quantifiable in monetary terms,
- Attainable: Achievable through best efforts,
- Relevant: Entity must be in need of these, and
- Timely: Achieved within a given time frame.

BPA Implementation

Step 5: Engage the business process consultant- To decide as to which company/ consultant to partner with, depends upon the following:

♦ Objectivity of consultant in understanding/evaluating entity situation.

♦ Does the consultant have experience with entity business process?

♦ Is the consultant experienced in resolving critical business issues?

♦ Whether the consultant can recommend and implementing a combination of hardware, software and services as appropriate to meeting enterprise BPA requirements?

♦ Does the consultant have the required expertise to clearly articulate the business value of every aspect of the proposed solution?

BPA Implementation

Step 6: Calculate the RoI for project

The right stakeholders need to be engaged and involved to ensure that the benefits of BPA are clearly communicated and implementation becomes successful. Hence, the required business process owners have to be convinced so as to justify the benefits of BPA and get approval from senior management.

BPA Implementation

Step 7: Developing the BPA

Once the requirements have been document, ROI has been computed and top management approval to go ahead has been received, the consultant develops the requisite BPA. The developed BPA needs to meet the objectives for which the same is being developed.

BPA Implementation

Step 8: Testing the BPA

Once developed, it is important to test the new process to determine how well it works and identify where additional “exception processing” steps need to be included. The process of testing is an iterative process, the objective being to remove all problems during this phase.

Case 1: Automation of purchase order process in an manufacturing entity: **From MODULE**

Case 2: Employee Attendance Automation: **From MODULE**

Case 3: Automation of internal audit process

Topics: MAIN

- Introduction
- Enterprise Business Processes
- Automated Business Processes
- Risk and Its Management
- Enterprises Risk Management
- Controls
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

Risk and Its Management

Introduction

- Sources
- Types
- Risk Management and Related Terms
- Risk Management Strategies

Risk and Its Management

- INTRODUCTION

- **Risk** is any event that may result in a significant deviation from a planned objective resulting in an unwanted negative consequence. The planned objective could be any aspect of an enterprise's strategic, financial, regulatory and operational processes, products or services. The degree of risk associated with an event is determined by the likelihood (uncertainly, probability) of the event occurring, the consequence (impact) if the event were to occur and it’s timings.

Risk and Its Management

- Introduction
- Sources
- Types
- Risk Management and Related Terms
- Risk Management Strategies

Sources

- *The most important step in risk management process is to identify the sources of risk, the areas from where risks can occur. This will give information about the possible threats, vulnerabilities and accordingly appropriate risk mitigation strategy can be adapted. Some of the common sources of risk are Commercial and Legal Relationships, Economic Circumstances, Human Behavior, Natural Events, Political Circumstances, Technology and Technical Issues, Management Activities and Controls, and Individual Activities.*
- **Broadly, risk has the following characteristics:**
  - *Potential loss that exists as the result of threat/vulnerability process;*
  - *Uncertainty of loss expressed in terms of probability of such loss; and*
  - *The probability/likelihood that a threat agent mounting a specific attack against a particular system.*

Risk and Its Management

- Introduction
- Sources
- Types
- Risk Management and Related Terms
- Risk Management Strategies

Types of Risks

- Business Risks
- Technological Risks
- Data Related Risks

Business Risks

- Businesses face all kinds of risks related from serious loss of profits to even bankruptcy and are discussed below:
  - *A) <u>Strategic Risk:</u> It includes reputation risk, leadership risk, brand risk, and changing customer needs.*
  - *B) <u>Financial Risk:</u> Examples include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.*
  - *C) <u>Regulatory (Compliance) Risk:</u> Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.*
  - *D) <u>Operational Risk:</u> Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.*

Type of Risks: Business Risks

- Businesses face all kinds of risks related from serious loss of profits to even bankruptcy and are discussed below:
  - *A) Strategic Risk: It includes reputation risk, leadership risk, brand risk, and changing customer needs.*
  - *B) Financial Risk: Examples include risks from volatility in foreign currencies, interest rates, and commodities; credit risk, liquidity risk, and market risk.*
  - *C) Regulatory (Compliance) Risk: Risk that could expose the organization to fines and penalties from a regulatory agency due to non-compliance with laws and regulations.*
  - *D) Operational Risk: Risk that could prevent the organization from operating in the most effective and efficient manner or be disruptive to other operations.*

Type of Risks: Business Risks

- E) Hazard Risk: Risks that are insurable, such as natural disasters; various insurable liabilities; impairment of physical assets; terrorism etc

- F) Residual Risk: Left over even after implementing counter measures.

MCQ 3:

CORONA / COVID is best example of a

a. Technology Risk

b. Data Risk

c. Business Risk

d. None of above

C

MCQ 4:

CORONA / COVID is which type of business risk

a. Financial Risk

b. Hazard Risk

c. Regulatory Risk

d. Operational Risk

B

Types of Risks

- Business Risks
- Technological Risks
- Data Related Risks

Types of Risks: Technological Risks

- The dependence on technology in BPA for most of the key business processes has led to various challenges. As Technology is taking new forms and transforming as well, the business processes and standards adapted by enterprises should consider these new set of IT risks and challenges: It includes
  - *Downtime due to technology failure*
  - *Frequent changes or obsolescence of technology:*
  - *Multiplicity and complexity of systems:*
  - *Different types of controls for different types of technologies/systems:*
  - *Proper alignment with business objectives and legal/regulatory requirements*
  - *Dependence on vendors due to outsourcing of IT services:*

Types of Risks: Technological Risks…2

- *Vendor related concentration risk:*
- *Segregation of Duties (SoD):*
- *External threats leading to cyber frauds/ crime:.*
- *Higher impact due to intentional or unintentional acts of internal employees:.*
- *New social engineering techniques employed to acquire confidential credentials:*
- *Need for governance processes to adequately manage technology and information security:*
- *Need to ensure continuity of business processes in the event of major exigencies*

Types of Risks

- Business Risks
- Technological Risks
- Data Related Risks

Types of Risks: Data Risks

- These include Physical access of data and Electronic access of data. (these are well explained in Chapter 3)

Risk and Its Management

- Introduction
- Sources
- Types
- **Risk Management and Related Terms**
- Risk Management Strategies

Risk Management and Related Terms

- **Risk Management:** Risk Management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources.
- **Asset**: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees. they all have one or more of the following characteristics:
  - *They are recognized to be of value to the organization.*
  - *They are not easily replaceable without cost, skill, time, resources or a combination.*
  - *They form a part of the organization's corporate identity, without which, the organization may be threatened.*
  - *Their data classification would normally be Proprietary, Highly confidential or even Top Secret.*

Risk Management and Related Terms..2

- **Vulnerability:** Vulnerability is the weakness in the system safeguards that exposes the system to threats. It may be a weakness in information system/s, cryptographic system (security systems), or other components (e.g. system security procedures, hardware design, internal controls) that could be exploited by a threat. Vulnerabilities potentially “allow” a threat to harm or exploit the system.
- **Threat**: Any entity, circumstance, or event with the potential to harm the software system or component through its unauthorized access, destruction, modification, and/or denial of service is called a Threat.

Risk Management and Related Terms..2

- **Exposure:** An exposure is the extent of loss the enterprise has to face when a risk materializes. It is not just the immediate impact, but the real harm that occurs in the long run. For example - loss of business, failure to perform the system's mission
- **Likelihood:** Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event.
- **Attack:** Anything that may hit on three pillars CIA.
- **Counter Measure:** An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure

MCQ 5:

Which if assessed poorly will lead to maximum loss

a. Vulnerability

b. Threat

c. Risk

d. Impact

A

Risk and Its Management

- Introduction
- Sources
- Types
- Risk Management and Related Terms
- **Risk Management Strategies**

Risk Management Strategies

- Effective risk management begins with a clear understanding of an enterprise's risk appetite and identifying high-level risk exposures. After defining risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Based on the type of risk, project and its significance to the business; Board and Senior Management may choose to take up any of the following risk management strategy in isolation or combination as required:

Risk Management Strategies

- **Tolerate/Accept the risk.** Some risks may be considered minor because their impact and probability of occurrence is low. In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.
- **Terminate/Eliminate the risk.** It is possible for a risk to be associated with the use of a technology, supplier, or vendor.
- **Transfer/Share the risk**: Risk mitigation approaches can be shared with trading partners and suppliers.
- **Treat/mitigate the risk;** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.
- **Turn back**; Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

MCQ 6: Which risk management strategy indicates lowest risk value

- A. Acceptance
- B. Termination
- C. Transferring
- D. Turn Back
- Answer : D

Topics: MAIN

- Introduction
- Enterprise Business Processes
- Automated Business Processes
- Risk and Its Management
- **Enterprises Risk Management**
- Controls
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

Enterprise Risk Management

- Introduction
- Benefits of ERM
- ERM Framework

Enterprise Risk Management: Introduction

- In implementing controls, it is important to adapt a holistic and comprehensive approach. Hence, ideally it should consider the overall business objectives, processes, organization structure, technology deployed and the risk appetite. Based on this, overall risk management strategy has to be adapted, which should be designed and promoted by the top management and implemented at all levels of enterprise operations as required in an integrated manner. Regulations require enterprises to adapt a risk management strategy, which is appropriate for the enterprise.
- Enterprise Risk Management (ERM) may be defined as a process, affected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Enterprise Risk Management: Benefits

No entity operates in a risk-free environment and ERM does not create such an environment. Rather, it enables management to operate more effectively in environments filled with risks. ERM provides enhanced capability to do the following:

- ❑ **Align risk appetite and strategy:** Risk appetite is the degree of risk, on a broad-based level that an enterprise (any type of entity) is willing to accept in pursuit of its goals. Management considers the entity's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy and in developing mechanisms to manage the related risks.

Enterprise Risk Management: Benefits…2

- ❑ **Link growth, risk and return:** Entities accept risk as part of value creation and preservation, and they expect return commensurate with the risk. ERM provides an enhanced ability to identify and assess risks, and establish acceptable levels of risk relative to growth and return objectives.
- ❑ **Enhance risk response decisions:** ERM provides the rigor to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance. ERM provides methodologies and techniques for making these decisions.
- ❑ **Minimize operational surprises and losses:** Entities have enhanced capability to identify potential events, assess risk and establish responses, thereby reducing the occurrence of surprises and related costs or losses.

Enterprise Risk Management: Benefits…3

- ❑ **Identify and manage cross-enterprise risks:** Every entity faces a myriad of risks affecting different parts of the enterprise. Management needs to not only manage individual risks, but also understand interrelated impacts.
- ❑ **Provide integrated responses to multiple risks:** Business processes carry many inherent risks, and ERM enables integrated solutions for managing the risks.
- ❑ **Seize opportunities:** Management considers potential events, rather than just risks, and by considering a full range of events, management gains an understanding of how certain events represent opportunities.
- ❑ **Rationalize capital:** More robust information on an entity’s total risk allows management to more effectively assess overall capital needs and improve capital allocation.

Enterprise Risk Management: Framework

- ERM provides a framework for risk management which typically involves identifying events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and pro-actively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.
- ERM framework consists of **eight** interrelated components that are derived from the way management runs a business, and are integrated with the management process. ***These components detailed in next slide***.

Enterprise Risk Management: Framework..2

1. **Internal Environment:** The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity’s people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. Management sets a philosophy regarding risk and establishes a risk appetite.
2. **Objective Setting:** Objectives should be set before management can identify events potentially affecting their achievement.
3. **Event Identification:** Potential events that might have an impact on the entity should be identified. Event identification includes identifying factors – internal and external – that influence how potential events may affect strategy implementation and achievement of objectives.

Enterprise Risk Management: Framework..3

4. Risk Assessment: Identified risks are analyzed to form a basis for determining how they should be managed. Risks are associated with related objectives that may be affected. Risks are assessed on both an inherent and a residual basis, and the assessment considers both risk likelihood and impact.

5. Risk Response: Management selects an approach or set of actions to align assessed risks with the entity's risk tolerance and risk appetite, in the context of the strategy and objectives. Personnel identify and evaluate possible responses to risks, including avoiding, accepting, reducing and sharing risk.

Enterprise Risk Management: Framework..4

6. Control Activities: Policies and procedures are established and executed to help ensure that the risk responses that management selected, are effectively carried out.

7. Information and Communication: Information is needed at all levels of an entity for identifying, assessing and responding to risk. Effective communication also should occur in a broader sense, flowing down, across and up the entity. Personnel need to receive clear communications regarding their role and responsibilities.

8. Monitoring: The entire ERM process should be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant

Topics: MAIN

- Introduction
- Enterprise Business Processes
- Automated Business Processes
- Risk and Its Management
- Enterprises Risk Management
- **Controls**
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

Controls

- Introduction
- Importance of IT Controls
- Applying IT Controls
- Indicators of Effective Controls
- Framework for Internal Controls as per Standards on Auditing

Controls: Introduction

- Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.

- Examples from MODULE

Controls: Introduction

- Control is defined as policies, procedures, practices and organization structure that are designed to provide reasonable assurance that business objectives are achieved and undesired events are prevented or detected and corrected.
  - <u>Examples from module</u>
    - Purchase
    - Sales
    - Goods Dispatch and 1000s more...

Controls: Introduction

- Types: Please open diagram in MODULE
  - Manual Control: Manually verify that the goods ordered in PO (A) are received (B) in good quality and the vendor invoice (C) reflects the quantity and price that are as per the PO (A).
  - Automated Control: The above verification is done automatically by the computer system by comparing (D), (E) & (F) and exceptions highlighted.
  - Semi-Automated Control: Verification of Goods Receipt (E) with PO (D) could be automated but the vendor invoice matching could be done manually in a reconciliation process (G).

MCQ 7: Home water filter intimating the service center on by its own self (IOT) on reduced levels of filtering resins is a good example of…

- A. Manual Controls
- B. Semi Automated Controls
- C. Automated Controls
- D. All of Above
- Answer : C

Controls

- Introduction
- Importance of IT Controls
- Applying IT Controls
- Indicators of Effective Controls
- Framework for Internal Controls as per Standards on Auditing

Controls: Importance

- IT Control objectives is defined as: 'a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity". Implementing right type of controls is responsibility of management. Controls provide a clear policy and good practice for directing and monitoring performance of IT to achieve enterprise objectives. IT Controls perform dual role:
  - They enable enterprise to achieve objectives; and
  - They help in mitigating risks.

Controls

- Introduction
- Importance of IT Controls
- **Applying IT Controls**
- Indicators of Effective Controls
- Framework for Internal Controls as per Standards on Auditing

Controls: Applying IT Controls

- Introduction
- Classification
  - *General Controls*
  - *Application Controls*

Controls: Applying IT Controls

- It is important for an organization to identify controls as per policy, procedures and its structure and configure it within IT software as used in the organization.
- There are different options for implementing controls as per risk management strategy. For example, the way banking is done in a nationalized bank is traditional way with rigid organization structure of managers at different levels, officers and clerks and clear demarcation between departments and functions whereas in a private sector, the organization structure is organized around customers and focused on relationship banking.

Controls: Applying IT Controls: Types

- **General Controls-** General Controls are macro in nature and the impact pervades the IT environment at different layers.

- **Application Controls-**Application Controls are controls which are specific to the application software.

Applying IT Controls: General Controls

- Information Security Policy:
- Administration, Access, and Authentication:
- Separation of key IT functions:
- Management of Systems Acquisition and Implementation:
- Change Management:
- Backup, Recovery and Business Continuity:
- Proper Development and Implementation of Application Software:
- Confidentiality, Integrity and Availability of Software and data files:
- Incident response and management:
- Value Add areas of Service Level Agreements (SLA):….**not an exhaustive list**

MCQ 8: A company is not having regular data back ups. This may reflect poor..

- A. Policy
- B. Performance
- C. Both a and b
- D. None of Above
- Answer : C

Applying IT Controls: Application Controls

- *Application Controls are controls which are implemented in an application to prevent or detect and correct errors. These controls are in-built in the application software to ensure accurate and reliable processing. These are designed to ensure completeness, accuracy, authorization and validity of data capture and transaction processing.*

- ***Some examples of Application controls on next slide:***

Applying IT Controls: Application Controls

- **Some examples of Application controls are as follows:**

- Data edits (editing of data is allowed only for permissible fields);
- Separation of business functions (e.g., transaction initiation versus authorization);
- Balancing of processing totals (debit and credit of all transactions are tallied);
- Transaction logging (all transactions are identified with unique id and logged);
- Error reporting (errors in processing are reported); and
- Exception Reporting (all exceptions are reported).

MCQ 9: Debtors with Credit Balance is best classified as..

- A. Normal
- B. Error
- C. Important
- D. Exception
- Answer : D

Controls

- Introduction
- Importance of IT Controls
- Applying IT Controls
- Indicators of Effective Controls
- Framework for Internal Controls as per Standards on Auditing

Controls: Indicators of Effective Control

- The ability to execute and plan new work such as IT infrastructure upgrades
- required to support new products and services.
- Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.
- Ability to allocate resources predictably.
- Heightened security awareness on the part of the users and a security conscious culture.

Controls: Indicators of Effective Control..2

- Consistent availability and reliability of information and IT services.
- Clear communication to management of key indicators of effective controls.
- The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently.
- - The efficient use of a customer support center or help desk.
- - Heightened security awareness on the part of the users and a security conscious culture.

Controls

- Introduction
- Importance of IT Controls
- Applying IT Controls
- Indicators of Effective Controls
- Framework for Internal Controls as per Standards on Auditing

SA 315

- SA 315 defines the system of Internal Control as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives regarding reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations.

Internal Control System

- Facilitates the effectiveness and efficiency of operations.
- Helps ensure the reliability of internal and external financial reporting.
- Assists compliance with applicable laws and regulations.
- Helps safeguarding the assets of the entity.

Internal Control Components

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring of Controls

Internal Control Components
I. Control Environment

- The Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. The Board of Directors and Senior Management establish the tone at the top regarding the importance of internal control, including expected standards of conduct. Management reinforces expectations at the various levels of the organization. The control environment comprises the integrity and ethical values of the organization; the parameters enabling the board of directors to carry out its governance responsibilities; the organizational structure and assignment of authority and responsibility; the process for attracting, developing, and retaining competent individuals; and the rigor around performance measures, incentives, and rewards to drive accountability for performance. The resulting control environment has a pervasive impact on the overall system of internal control.

Internal Control Components
II. Risk Assessment

- Every entity faces a variety of risks from external and internal resources. Risk may be defined as the possibility that an event will occur and adversely affect the achievement of objectives. **Risk Assessment** involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances.
- Thus, Risk Assessment forms the basis for determining how risks will be managed. A precondition to risk assessment is the establishment of objectives, linked at different levels of the entity. Management specifies objectives within categories of operations, reporting, and compliance with sufficient clarity to be able to identify and assess risks to those objectives. Risk assessment also requires management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.

Internal Control Components
III. Control Activities

- Control Activities are the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out. Control activities are performed at all levels of the entity, at various stages within business processes, and over the technology environment. They may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorizations and approvals, verifications, reconciliations and business performance reviews

Internal Control Components
IV. Information and Communication

- Information is necessary for the entity to carry out internal control responsibilities in support of the achievement of its objectives. Management obtains or generates and uses relevant and quality information from both internal and external sources to support the functioning of other components of internal control. Communication is the continual, iterative process of providing, sharing, and obtaining necessary information. Internal communication is how information is disseminated throughout the enterprise, flowing up, down, and across the entity. It enables personnel to receive a clear message from senior management that control responsibilities should be taken seriously. External communication is two-fold: it enables inbound communication of relevant external information and provides information to external parties in response to requirements and expectations.

Internal Control Components
V. Monitoring of Controls

- Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component is present and functioning. Ongoing evaluations built into business processes at different levels of the entity, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against

Internal Control Components
Limitations of Internal Control System

- Internal control systems are subject to certain inherent limitations, such as:
  - *Management's consideration that the cost of an internal control does not exceed the expected benefits to be derived.*
  - *The fact that most internal controls do not tend to be directed at transactions of unusual nature.*
  - *The possibility of circumvention of internal controls through collusion with employees or with parties outside the entity.*
  - *The possibility that a person responsible for exercising an internal control could abuse that responsibility, for example, a member of management overriding an internal control.*
  - *Manipulations by management with respect to transactions or estimates and judgments required in the preparation of financial statements.*

Topics: MAIN

- Introduction
- Enterprise Business Processes
- Automated Business Processes
- Risk and Its Management
- Enterprises Risk Management
- Controls
- Diagrammatic Representation of Business Processes
- Risks and Controls for Specific Business Processes
- Regulatory and Compliance Requirements

FLOWCHART

- Flowchart 1: Add three numbers A B C and Print the Result.
- Flowchart 2: Identify highest from three numbers A, B, C
- Flowchart 3: Add first 25 even numbers and print the result.

THANK YOU