



Date: 03 April 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

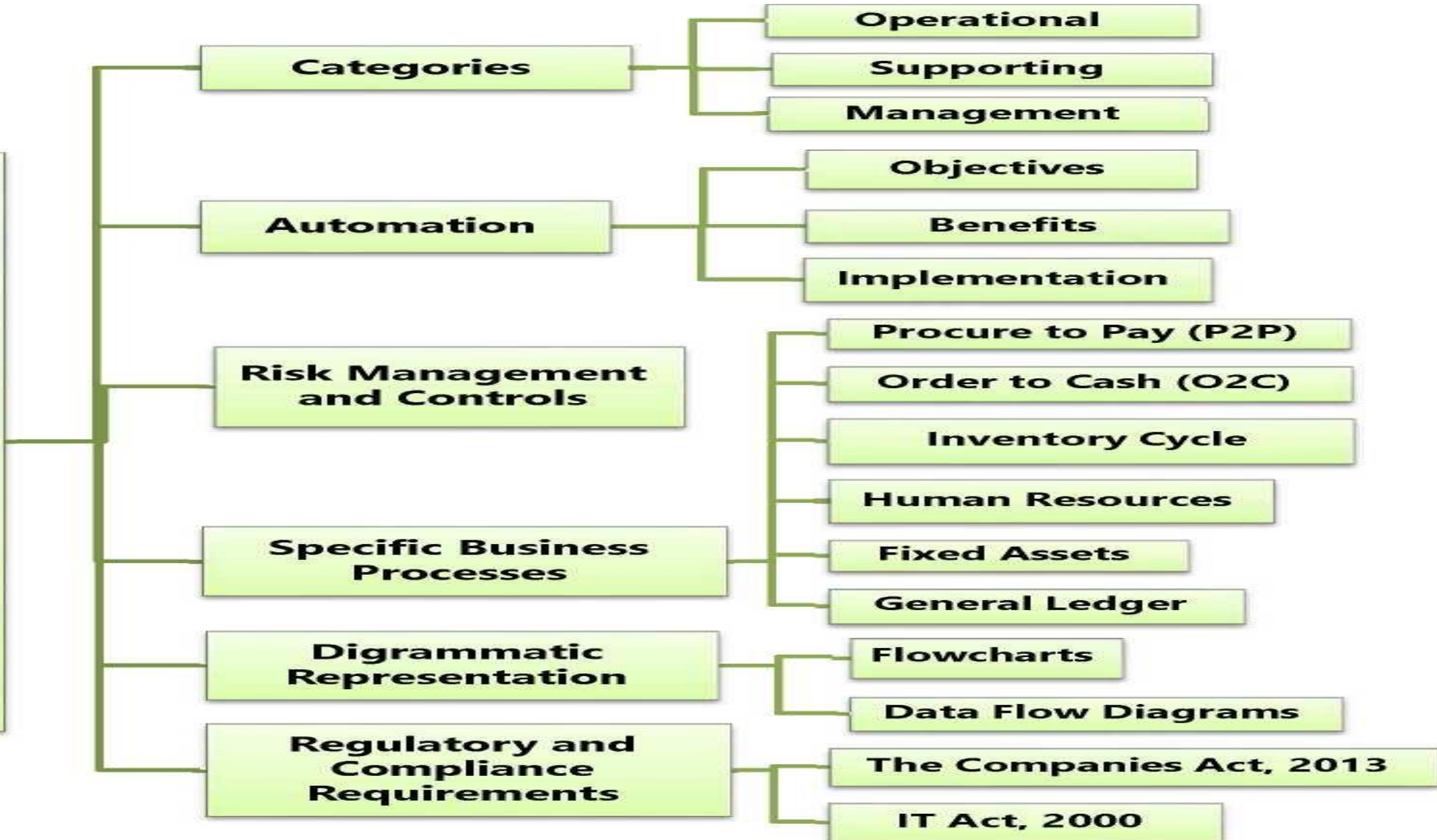
- You all have been through many sessions and you realize that subject is absolutely practical....



Starting with

- Chapter 1: Automated Business Process

Enterprise Business Processes



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.

Topics: MAIN

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

Risk & Controls for Specific Business Processes

- Suitable controls should be implemented to meet the requirements of the control objectives. These controls can be manual, automated or semi-automated provided the risk is mitigated. Based on the scenario, the controls can be Preventive, Detective or Corrective. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction. In computer systems, controls should be checked at three levels, namely
 - Configuration,
 - Masters and
 - Transaction level.

Configuration

- Configuration refers to the way a software system is set up. Configuration is the methodical process of defining options that are provided. When any software is installed, values for various parameters should be set up (configured) as per policies: Some examples of configuration:
 - Mapping of accounts to front end transactions like purchase and sales
 - Control on parameters: Creation of Customer Type, Vendor Type, year-end process
 - User activation and deactivation
 - User Access & privileges - Configuration & its management
 - Password Management

Masters

- Masters refer to the way various parameters are set up for all modules of software, like Purchase, Sales, Inventory, and Finance etc. These drives how the software will process relevant transactions. The masters are set up first time during installation and these are changed whenever the business process rules or parameters are changed. Some examples are
 - *Vendor Master*
 - *Customer Master*
 - *Material Master*
 - *Employee Master*

Masters

- Vendor Master: Credit period, vendor bank account details, etc.
- Customer Master: Credit limit, Bill to address, Ship to address, etc.
- Material Master: Material type, Material description, Unit of measure, etc.
- Employee Master: Employee name, designation, salary details, etc.

Masters

- Vendor Master: Credit period, vendor bank account details, etc.
- Customer Master: Credit limit, Bill to address, Ship to address, etc.
- Material Master: Material type, Material description, Unit of measure, etc.
- Employee Master: Employee name, designation, salary details, etc.

Transaction: From Module

- Procure to Pay
- Order to Cash
- Inventory Cycle
- Human Resources
- Fixed Assets
- General Ledger

Topics: MAIN

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

DIAGRAMMATIC REPRESENTATION OF BUSINESS PROCESSES

LAST PART OF LECTURE

Topics: MAIN

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

Regulations

- Companies Act 2013
 - ICAI Mandates
 - Corporate Governance Requirements
 - Information Technology Act, 2008
-
- All from MODULE

FLOW CHARTS

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