CA Final: Summary Notes on

Information Systems Control and Audit (ISCA)

ISCA

Quick Revision Points

Sumit Shanker Dandowtiya

(FCA, DISA, CISA)

Course Duration: Two month / 48 Lectures Approx.
For new batch announcement check www.cafinal.com

www.cafinal.com

QRP
May 16

Where the mind is without fear

Where the mind is without fear and the head is held high
Where knowledge is free
Where the world has not been broken up into fragments
By narrow domestic walls
Where words come out from the depth of truth
Where tireless striving stretches its arms towards perfection
Where the mind is led forward by thee
Into ever-widening thought and action
Into that heaven of freedom, my Father, let my country awake

- Rabindranath Tagore

ISCA Lecture Schedule

(Total Duration: Two Months / 48 Lectures Approx.)

Chapter		Start Date	Finish Date	Duration (48 Lectures)
Ch 1*	*Concepts of Governance and Management of Information Systems*			
Ch 2*	*Information Systems Concepts*			
Ch 3*	*Protection of Information Systems*			
Ch 4*	*Business Continuity and Disaster Recovery Planning*			
Ch 5*	*Acquisition, Development and Implementation of Information Systems*			
Ch 6*	*Auditing of Information Systems*			
Ch 7*	*Information Technology Regulatory Issues*			
Ch 8*	*Emerging Technologies*			

Morning batch: 10.15 – 11.30 AM (Apr-May, Aug-Sep, Dec-Jan)

Evening batch: 5.30 – 6.45 PM (Feb-Mar, Jun-Jul, Oct-Nov)

Address: 17, Luv-Kush Nagar (First),
Near JP Underpass, Sahakar Marg, Jaipur

Ph: 9314207273

* References – Final Course Study Material, Information Systems Control and Audit, ICAI.

Strategy for winning in ISCA

1. *Consistency: Give time to this subject on regular basis, just 45 minutes, but daily. Do not leave this subject for last month preparation.*

2. *Keep Writing: Learn by writing bullet points again and again. Writing will make it easier to remember the points.*

3. *Revise: This subject requires repeated revision.*

4. *Conceptual Understanding: This subject requires both learning + conceptual understanding. Learning helps to answer the questions in exam but learning cannot be done without conceptual understanding.*

5. *Mock Test: Please appear for mock test one month before exam. This will help you to gauge your performance well in advance.*

6. *In Exam: Read the question very carefully in exam to identify and locate the correct chapter and paragraph. Misidentification is the major reason for securing less marks in this subject.*

Wish you all the best

CA Sumit Shanker

17 Luv-Kush Nagar – I
Sahakar Marg,
Jaipur - 302015

Important: This book is only meant for revision purpose. For detail discussion please refer comprehensive notes on ISCA by Sumit Shanker.

CHAPTER 1 – QRP

Concepts of Governance and Management of Information Systems

Key Topics:

1. Governance and Internal Control
2. IT Strategy Planning
3. Risk Management
4. COBIT 5 and IT Compliance Review

◙ Key concepts of Governance:

1. *Governance*:
   - means to steer or control any system
   - evaluating, directing and monitoring performance.
2. *Enterprise Governance*:
   - means the mechanism used by the top management to direct and control enterprise.
3. *Corporate Governance*:
   - means the system by which a company is directed and controlled
   - it includes the structure and process for the direction and control of companies.

◙ Corporate Governance and IT Governance

Benefits of Governance: Major benefits of governance can be summarized as follows:

i) *Achieving enterprise objectives*
ii) *Transparent framework for decision making*
iii) *Desirable behavior in the use of IT*
iv) *Desired business processes*
v) *Providing stability in* organization
vi) *Improving customer* satisfaction
vii) *Effective and strategically aligned decision making*

Governance Dimensions

1) Conformance **(***Corporate Governance Dimension***)**	2) ***Performance*** *(Business Governance Dimension*)
o provides a *historic view* o *focuses on regulatory requirements*. o covers the *roles of the chairman, CEO and BOD* o covers *audit and assurance* o *oversight mechanisms*	o provides *pro-active* view o *business oriented view* o *forward looking view* o focuses on *strategy* and value creation o understand risk

◙ IT Governance and GEIT:

IT Governance: IT Governance refers to the system in which directors of the enterprise evaluate, direct and monitor IT management to ensure effectiveness, accountability and compliance of IT.

Key practices to determine status of IT Governance: *Some of the key practices, which determine the status of IT Governance in the enterprise, are:*

- Who makes directing, controlling and executing decisions?
- How the decisions are made?
- What information is required to make the decisions?
- What decision-making mechanisms are required?
- How exceptions are handled?
- How the governance results are monitored and improved?

Benefits of IT Governance

- Increased *value* delivered through enterprise IT
- Increased *user satisfaction* with IT services
- Improved *agility* in supporting business needs
- Better *cost* performance of IT
- Improved management and mitigation of *IT-related business risk*
- IT becoming an *enabler for change* rather than hindrance
- Improved *transparency* and understanding of IT's contribution to the business
- Improved *compliance* with relevant laws, regulations and policies; and
- More *optimal utilization* of IT resources.

For every defined benefit, it is critical to ensure that:

- Ownership is defined and agreed
- It is relevant and links to the business strategy
- The timing of its realization of benefit is realistic and documented
- The risks, assumptions and dependencies are understood, correct and current
- An unambiguous measure has been identified; and
- Timely and accurate data for the measure is available or is easy to obtain.

Governance of Enterprise IT (GEIT): *The primary objective of GEIT is to analyze the requirements for the governance of enterprise IT, and to put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.*

Benefits of GEIT

- Consistent approach integrated and aligned with the enterprise governance approach
- IT-related decisions are made in line with the enterprise's strategies and objectives
- IT-related processes are overseen effectively and transparently
- Compliance with legal and regulatory requirements
- Governance requirements for board members are met

Key governance practices of GEIT

i) ***Evaluate*** *the Governance System*
ii) ***Direct*** *the Governance System*
iii) ***Monitor*** *the Governance System*

◙ Corporate Governance, ERM and Internal Controls

Some of the best practices of corporate governance are as follows:

- *Clear assignment of responsibilities* and decision-making authorities
- *Interaction and cooperation* among the BOD, senior management and the auditors
- *Strong internal control systems*
- Independent internal and external audit functions
- Monitoring of *conflicts of interest*
- Financial and managerial *incentives* to act in an appropriate manner
- *Information flows* internally and to the public.

ERM: Enterprise Risk Management

- Before implementing controls it is important to consider the overall business risk
- Sarbanes Oxley Act (SOX) in the US focuses on the implementation and review of internal controls
- SOX has used COSO framework as a guide for implementing risk management and internal controls. *[COSO-Committee of Sponsoring Organizations of the Treadway Commission]*
- Definition of ERM: *"Enterprise risk management is a process, effected by board of directors, management and other personnel, applied in strategy setting 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."*

Internal Controls

(a) Responsibility for Implementing Internal Controls: Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) personally and criminally liable for the quality and effectiveness of their organization's internal controls

(b) Internal Controls as per COSO: According to COSO, Internal Control is comprised of five interrelated components:

1. *Control Environment*
2. *Risk Assessment*
3. *Control Activities*
4. *Information and Communication*
5. *Monitoring*

(c) Clause 49 of the listing agreements issued by SEBI requires the implementation of enterprise risk management and internal controls and holds the senior management legally responsible for such implementation

◙ **Role of IT in Enterprises**

- o *Strategic and competitive advantage*
- o *Online services*
- o *Transform business process*
- o *Impact on internal controls*
- o *Organizational restructuring*

◙ **Business and IT Strategy**

- Management Strategy determines the overall path and methodology
- Strategy is formulated by the senior management
- There is a *fusion of IT strategy with business strategy*
- Every enterprise needs to have an internal control system
- Auditors could be involved in providing assurance and review of internal controls
- IT department should define their strategies and tactics to support the organization
- Metrics and goals are established to measure IT perform on a tactical basis

◙ **IT Steering Committee**: The senior management may appoint a high-level committee to provide appropriate direction for IT development. *The key functions of the Steering Committee would include of the following:*

- o To ensure that long and short-range *IT plans are in tune with enterprise* objectives
- o To establish *size and scope of IT function* and sets priorities
- o To *review and approve* major IT deployment projects in all their stages
- o To approve and *monitor key projects* by measuring result of IT projects in terms of ROI
- o To review the *status of IS plans and budgets* and overall IT performance
- o To review and approve *standards, policies and procedures*
- o To make *decisions on all key aspects* of IT deployment and implementation
- o To facilitate implementation of *IT security* within enterprise
- o To *resolve conflicts* in deployment of IT
- o To *report to the Board of Directors* on IT activities on a regular basis.

◙ **IT Strategy Planning**: *Planning* is basically deciding in advance '*what is to be done*', '*who is going to do*' and '*when it is going to be done*'. There are three levels of managerial activity in an enterprise:

- *Strategic Planning*: Planning done by top management
- *Management Control*: Process to assure that resources are used effectively
- *Operational Control*: Process to assure that specific tasks are carried out effectively and efficiently.

***IT Strategy planning in an enterprise could be classified into the following categories*:**

(i) *Enterprise Strategic Plan***:** It provides the overall direction, mission, strategic objectives, an assessment of environmental.

(ii) *Information Systems Strategic Plan***:** It focus on balancing IT opportunities and IT business requirements. Some of the enablers of the IS Strategic plan are:

- Enterprise business strategy
- Inventory of technological solutions
- Monitoring the technology markets
- Feasibility studies
- Existing systems assessments
- Enterprise position on risk, and
- Need for senior management support

(iii) *Information Systems Requirements Plan*: It defines information system architecture i.e. the major functions needed to support planning, control and operations activities. Some of the key enablers of the information architecture are:

- Automated data repository and dictionary
- Data syntax rules
- Data ownership and security classification
- An information model representing the business, and
- Enterprise information architectural standards.

(iv) *Information Systems Applications and Facilities Plan*: This plan includes:

- Specific application systems to be developed and an associated time schedule
- Hardware and Software acquisition/development schedule
- Facilities required, and
- Organization changes required.

◙ **Objectives of IT Strategy**:

The primary objective of IT strategy is:

- o To provide a *holistic view* of the current IT environment
- o To set the *future direction*,
- o To *take initiatives* required to shift to the desired future environment
- o To enable quick, reliable and *efficient response* to strategic objectives

Key Management practices for Aligning IT Strategies with Enterprise Strategy

i) *Understand enterprise direction*
ii) *Assess the current environment, capabilities and performance*
iii) *Define the target IT capabilities*
iv) *Conduct a gap analysis*
v) *Define the strategic plan and road map*
vi) *Communicate the IT strategy and direction*

◙ **Business Value from Use of IT**

i) *Evaluate Value Optimization*: Continually evaluate IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives

ii) *Direct Value Optimization*: Direct value management principles and practices to enable optimal value realization from IT enabled investments

iii) *Monitor Value Optimization*: Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise

Key metrics, which can be used for evaluation the transparency and IT benefits are:

- o Percentage of IT investments where benefit realization has been monitored through full economic life cycle
- o Percentage of IT services where expected benefits realized
- o Percentage of IT investments where claimed benefits achieved or exceeded
- o Percentage of business investments with clearly defined and approved expected IT related costs and benefits
- o Percentage of IT services with clearly defined and approved operational costs and expected benefits; and
- o Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial information.

___________x____________x____________

◙ IS Risk and Risk Management

Sources of Risk: 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.

Characteristics of Risk: Broadly, risk has the following characteristics:

- *Loss potential* that exists as the result of threat/vulnerability process
- *Uncertainty of loss* expressed in terms of probability of such loss; and
- *Likelihood of threat* agent causing a specific attack against a particular system.

Risk Related Terms

Asset: Asset can be defined as something of value to the organization. Characteristics of assets –

- Valuable to the organization
- Cannot be easily replaced without cost, skill, time, resources
- Part of the organization’s corporate identity
- Classified according to their criticality

Vulnerability: Vulnerability is the weakness in the system safeguards that exposes the system to threats. Some examples of vulnerabilities are given as follows:

- Leaving the front door unlocked makes the house vulnerable to unwanted visitors
- Short passwords (less than 6 characters) make the system vulnerable

Vulnerability exist when system has at least one condition, out of the following:

- Allows an attacker to execute commands as another user or
- Allows an attacker to access data that has access restrictions or
- Allows an attacker to pose as another entity or
- Allows an attacker to conduct a denial of service

Threat: Any entity, circumstance, or event with the potential to harm the system. Assets and threats are closely correlated. A threat cannot exist without a target asset.

Exposure: An exposure is the extent of loss the enterprise has to face when a risk materializes. It includes both immediate and long run impact.

Likelihood: Probability of occurrence of an undesirable event.

Attack: An attack is an attempt to gain unauthorized access into the system Basically, it is a set of actions designed to compromise CIA (Confidentiality, Integrity or Availability)

Risk: It is defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset

Risk analysis: It is defined as the process of identifying security risks and determining their magnitude and impact on an organization.

Risk assessment includes the followings:

- Identification of threats and vulnerabilities in the system
- Potential impact or degree of harm that a loss of CIA, would have on enterprise operations or assets, if a vulnerability is exploited by a threat, and
- The identification and analysis of security controls for the information system.

Information systems can generate many direct and indirect risks. These risks lead to a gap between the need to protect systems and the degree of protection applied. The gap between required and actual degree of protection is caused by:

- Widespread use of technology
- Interconnectivity of systems
- Elimination of distance, time and space as constraints
- Unevenness of technological changes
- Decentralization of management and control
- Attractiveness of conducting unconventional electronic attacks
- Weak legal and regulatory requirements

Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of system is referred as countermeasure.

*Residual Risk***:** Any risk still remaining after the counter measures are analyzed and implemented is called Residual Risk. The risk can be minimized, but it cannot be totally eliminated. Residual risk must be kept at a minimal, acceptable level.

Risk Management Strategies

1) *Tolerate/Accept the risk*: Accept some risk that are minor
2) *Terminate/Eliminate the risk*: If risk is associated with the use of a particular technology, supplier or vendor then risk can be eliminated by replacing them.
3) *Transfer/Share the risk*: Risk be shared with trading partners and suppliers by outsourcing the activities. Risk also may be mitigated by insurance.
4) *Treat/mitigate the risk*: Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from occurring or to minimize its effects.
5) *Turn back*: Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Key Governance Practices for Evaluating Risk Management

i) Evaluate Risk Management
ii) Direct Risk Management
iii) Monitor Risk Management

Key Management Practices for implementing Risk Management:

i) *Collect Data*
ii) *Analyze Risk*
iii) *Maintain a Risk Profile*
iv) *Articulate Risk*
v) *Define a Risk Management Action Portfolio*
vi) *Respond to Risk*

Metrics of Risk Management: key metrics for monitoring IT are:

- Percentage of critical business processes, IT services and IT-enabled business programs covered by risk assessment
- Number of significant IT related incidents that were not identified in risk Assessment
- Percentage of enterprise risk assessments including IT related risks; and
- Frequency of updating the risk profile based on status of risk assessment.

◙ COBIT 5 – A GEIT Framework

- COBIT: ***Control Objectives for Information and Related Technology***
- COBIT: Developed by "Information System Audit and Control Association" (ISACA) USA
- Latest version: COBIT 5 *(April 2012)*
- COBIT5 structure: Five principles and seven enablers

Need for Enterprise to Use COBIT 5

- *Globally accepted principles, practices, analytical tools*
- *Create optimal value for the organization*
- Provides tools to understand, utilize, implement and direct IT related activities
- *Make more informed decisions*
- Can be used by all types and size of enterprises, including nonprofit and public sector
- Benefits of using COBIT5:
  - i) Increased *value creation* from use of IT
  - ii) *User satisfaction* with IT engagement and services
  - iii) *Reduced IT related risks*
  - iv) Development of more *business-focused IT solutions* and services; and
  - v) Increased *enterprise wide involvement* in IT-related activities.

Integrating COBIT 5 with Other Frameworks: COBIT 5 is a comprehensive framework and is based on overall enterprise view and is aligned with enterprise governance best practices such as

- GEIT (Governance of Enterprise IT)
- ITIL
- TOGAF (The Open Group Architecture Framework)
- ISO 27000
- ISO 38500
- Val IT
- Risk IT

Components in COBIT

1) ***Framework*** - Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements
2) ***Process Descriptions*** - The processes map to responsibility areas of plan, build, run and monitor.
3) ***Control Objectives*** - Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.
4) ***Management Guidelines*** - Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes
5) ***Maturity Models*** - Assess maturity and capability per process and helps to address gaps.

Benefits of COBIT 5

- *Can be implemented in all sizes of enterprises*.
- Helps in *achieving their objectives* for the governance and management of enterprise IT.
- Helps enterprise to *create optimal value from IT*
- *Holistic approach*
- *Manage IT related risk* and *ensures compliance, continuity, security and privacy*.
- Enables *clear policy development*
- Generic framework
- *supports compliance* with relevant laws, regulations

Customizing COBIT 5 as per Requirement: COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

- Information security
- Risk management
- Governance and management of enterprise IT
- Assurance activities
- Legislative and regulatory compliance
- Financial processing or CSR reporting

Five Principles of COBIT 5:

Principle 1: Meeting Stakeholder Needs

- Enterprises has to create value for their stakeholders
- COBIT 5 provides the processes and enablers to support business value creation
- Enterprise can customize COBIT 5 to suit its own objectives

Principle 2: Covering the Enterprise End-to-End

- COBIT 5 integrates IT governance of enterprise into enterprise governance
- It considers all IT related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT

Principle 3: Applying a Single Integrated Framework

- Earlier, organizations had to follow many IT-related standards and best practices
- But now, COBIT 5 is a single and integrated framework

Principle 4: Enabling a Holistic Approach

- Efficient and effective governance and management require a holistic approach
- COBIT 5 defines a set of 7 enablers
- Enablers are defined as anything that helps in achieving the objectives of the enterprise.

Principle 5: Separating Governance from Management

- The COBIT 5 makes a clear distinction between governance and management
- **Governance**: Done by BOD and Chairperson
- **Management**: Done by executive management under the leadership of the CEO.

COBIT 5 Process Reference Model: COBIT 5 includes a Process Reference Model, which describes in details a number of governance and management processes of enterprise IT into two main process domains:

Governance Process:

- *Evaluate, Direct and Monitor Practices (EDM) – 5 processes*

Management Process:

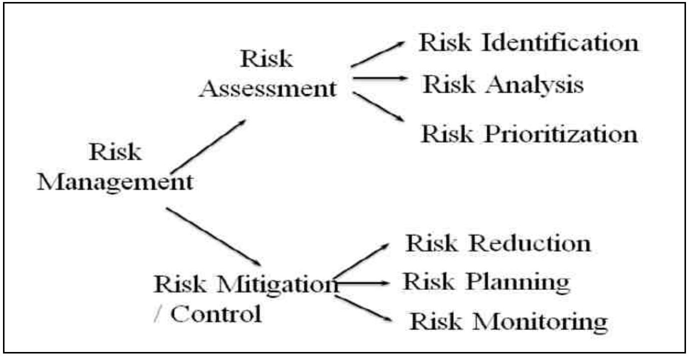
- *Align, Plan and Organize (APO) – 13 processes*
- *Build, Acquire and Implement (BAI) – 10 processes*
- *Deliver, Service and Support (DSS) – 6 processes*
- *Monitor, Evaluate and Asses (MEA) – 3 processes*

***Seven Enablers of COBIT 5*:**

1. Principles, policies and frameworks
2. Processes
3. Organizational structures
4. Culture, ethics and behavior
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

Risk Management in COBIT 5

A pictorial representation of various activities relating to risk management is given below



Using COBIT 5 Best practices for GRC: <u>GRC program implementation requires the following steps:</u>

- Defining GRC requirements in clear terms
- Identifying the regulatory and compliance requirements
- Reviewing the current GRC status
- Determining the most optimal approach
- Setting out key parameters for measurement of success
- Using a process oriented approach
- Adapting global best practices, and
- Using uniform and structured approach which can be audited

<u>Success of a GRC program can be measured by using the following goals and metrics:</u>

- Reduction of redundant controls
- Reduction in control failures in all key areas
- Reduction of expenditure relating to legal, regulatory and review areas
- Reduction in overall time required for audit for key business areas
- Streamlining of processes and automation of control and compliance measures
- Timely reporting of regular compliance issues and remediation measures
- Real-time dashboard of compliance status and key issues for senior management

◙ **IT Compliance Review:** Following are some of the regulatory/legal requirements for GRC (Governance, Risk Management and Compliance) in an enterprise:

- *<u>Sarbanes Oxley Act</u>*: Sarbanes Oxley Act of US has been passed to protect investors by improving the accuracy and reliability of corporate disclosures.
- *<u>Clause 49 of SEBI</u>*: Clause 49 mandates implementation of enterprise risk management and internal controls as appropriate for the enterprise

- *Information Technology Act*: It provides legal recognition for electronic records and also mandates responsibilities for protecting information. The Act also identifies various types of cyber-crimes and has imposed specific responsibilities on corporate.
- *CARO*: It is compulsory to reporting on Internal control and a separate annexure to the audit report has to be provided by auditors as per CARO 2003.
- *PCAOB*: In USA, the PCAOB has come out with detailed guidelines on Compliance by Auditors and Companies under the Act

Compliance in COBIT 5

- *MEA03: Monitor, Evaluate and Assess Compliance with External Requirements*
- RACI Chart *(Responsible, Accountable, Consulted or Informed)*
- *COBIT 5 Governance Domain*

Key Management Practices of IT Compliance:

i) *Identify External Compliance Requirements*
ii) *Optimize Response to External Requirements*
iii) *Confirm External Compliance*
iv) *Obtain Assurance of External Compliance*

Key Metrics for Assessing Compliance Process:

I. *Compliance with External Laws and Regulations*: These metrics are given as follows:
   - Cost of IT non-compliance, including settlements and fines
   - Number of IT related non-compliance issues reported
   - Number of non-compliance issues relating to contractual agreements
   - Coverage of compliance assessments.

II. *IT Compliance with Internal Policies*: These metrics are given as follows:
   - Number of incidents related to non-compliance to policy
   - Percentage of stakeholders who understand policies
   - Percentage of policies supported by effective standards and working practices
   - Frequency of policies review and updates.

◙ Information Systems Assurance

Using COBIT 5 for IS Assurance

- *Meet expectations of multiple stakeholders*
- Written in a *non-technical language*
- *Widely used with COSO* by management, IT professionals, regulators and auditors
- *Umbrella framework* under which other standards have been integrated.

Evaluating IT Governance Structure and practices by Internal Auditors: IT Governance can be evaluated by both external and internal auditor. The following guidance is issued by The Institute of Internal Auditors (IIA) from internal auditor perspective:

i) *Leadership*: Auditors review
- Evaluate the relationship between IT objectives and business objectives
- Assess the involvement of IT leaders
- Determine how effectiveness of IT will be measured in achieving the goals
- Review how roles and responsibilities are assigned within IT organization
- Review the role of senior management in maintaining strong IT governance

ii) *Organizational Structure*: Auditors review
- Review how the management and IT personnel are interacting and communicating.
- Review the existence of reporting relationships in IT department

iii) *Processes*: Auditors review
   - Evaluate IT processes and controls in place to mitigate risks
   - What processes are used by the IT organization to support the IT environment

iv) *Risks*: Auditors review
   - Review the processes used to identify, assess, and monitor/mitigate risks
   - Determine the accountability that personnel have within risk management.

v) *Controls*: Auditors review
   - Assess key controls that are designed by IT department to manage its activities
   - Ownership, documentation, and reporting should be reviewed by the internal auditor.
   - The controls should be strong enough to address identified risks.

vi) *Performance Measurement/Monitoring*: Auditors review
   - Evaluate the framework and systems in place to measure and monitor organizational performance from IT point of view.

Sample Areas of GRC for Review by Internal Auditorsas per IIA:

- Scope of audit
- Evaluate Governance
- Evaluate Enterprise Ethics
- Evaluate Risk Management
- Evaluate Risk Exposures
- Evaluate Fraud and Fraud Risk
- Address Adequacy of Risk Management Process

Sample Areas of Review of Assessing and Managing Risks

The specific areas evaluated by auditor are:

- Risk management *ownership and accountability*
- Different *kinds of IT risks* (technology, security, continuity, regulatory, etc.)
- Defined and communicated *risk tolerance profile*
- Root cause analyses and *risk mitigation measures*
- *Quantitative* and/or *qualitative risk measurement*
- *Risk assessment methodology*; and
- *Risk action plan* and *Timely reassessment*.

Evaluating and Assessing the System of Internal Controls as per COBIT 5:

COBIT 5 has specific process: "*MEA 02 Monitor, Evaluate and Assess the System of Internal Control*", which provides guidance on evaluating and assessing internal controls implemented in an enterprise.

The objective of such a review is to:

i) *Continuously monitor* and evaluate the control environment
ii) *Identify management deficiencies* and initiate improvement actions; and
iii) Plan, organize and maintain *standards for internal control* assessment

Key management practices for assessing and evaluating the system of internal controls are:

- *Continuously Monitor Internal Controls*
- *Review Business Process Controls Effectiveness*
- *Perform Control Self-assessments*
- *Identify and Report Control Deficiencies*
- *Ensure that assurance providers are independent and qualified*
- *Plan Assurance Initiatives* based on enterprise objectives
- *Scope assurance initiatives*
- *Execute assurance initiatives*

CHAPTER 2 – QRP

Information Systems Concepts

Key Topics:

1. Overview of Information Systems
2. Types of Information System
3. Application of Information Systems in Enterprise Processes
4. Information as a Key Business Asset and its Relation to Business Objectives and Processes
5. Various types of Business Applications
6. Overview of Underlying IT Technologies

1. Overview of Information Systems

◙ ***Information System***: Information system is a system that comprises of people, computer systems, data and network that helps to collect, store and analyze data to produce the desired information for the functioning, betterment and expansion of business.

◙ ***Information***: Information means processed data

◙ ***Date***: Data is raw collection of facts or events, E.g. In a spread sheet having students name, roll number and marks obtained in science, Hindi, English subject represents data, whereas average marks of all students in a subject is information.

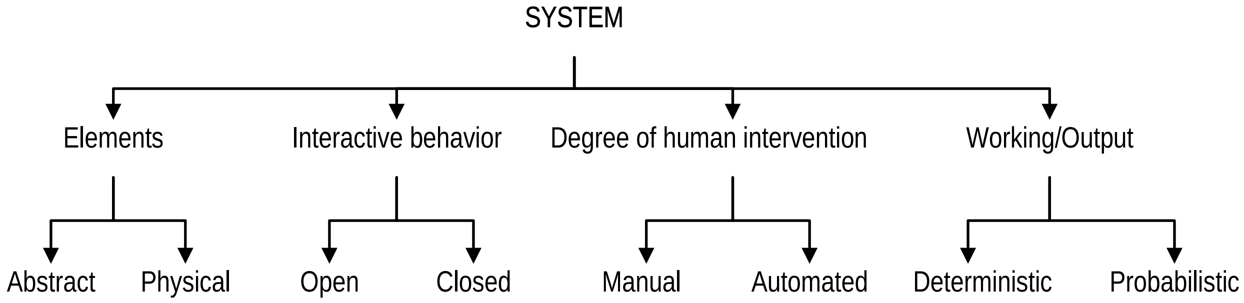
◙ **Attributes (Characteristics) of information:**

1. Availability
2. Purpose
3. Mode and format
4. Updated
5. Rate
6. Frequency
7. Completeness
8. Reliability
9. Validity
10. Quality
11. Transparency
12. Value of information

◙ **System:**

- System means a set of interrelated elements that operate collectively to accomplish some common object
- It takes input from its environment and returns output again to the environment.

◙ General classification of system:



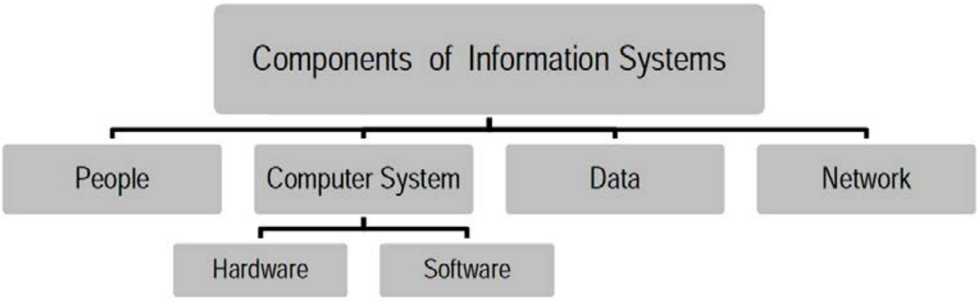
I. Classification of system based on "Elements"	
Physical system	Abstract system
- can be seen and touched. - Eg: Transport, computer, business system etc - can be of different size and serve different purpose	- cannot be seen and touched - can only be visualized by our mind. - Eg: system of religious beliefs, theology - Eg: Diagrams and flowcharts

II. Classification of system based on "Interactive behavior"	
Open system	Closed system
- takes input from its environment and returns some output to the environment. - change and adapt according to the environment - Eg: Business, Marketing, communication system etc	- does not interact with the environment - does not change according to the environment - can only be relatively closed - Eg production system, computer system. - E.g. "use and throw" sealed digital watch

III. Classification of system based on "Human intervention"	
Manual system	Automated system
- work done by human efforts. - Eg: Manual accounting system	- computer system is used to carry out the entire task - human intervention is nil or very less. - some manual intervention is always there - E.g. auto-pilot aviation, software controlled processes, business ERP system.

IV. Classification of system based on "Working/Output"	
Deterministic system	Probabilistic system
- gives exact output. - operate in a predictable manner - behavior of the system is known with certainty - Eg: accounting information system, communication system, computer system, production system etc.	- provide expected output. - uncertainty about the outcome and behavior - for a given set of input, the output cannot be known with certainty - Eg: weather forecasting system, sales forecasting system, pricing system, inventory management system, marketing system etc.

◙ ***Components of Information Systems***



An information system model comprises of the following steps:
Step 1: Data is collected and converted into suitable format for input
Step 2: Data is processed and converted into information
Step 3: Information is stored for future use or communicated to user

Characteristics of Computer Based Information Systems are as follows:

1) Predetermined objectives
2) Interrelated and interdependent subsystems
3) Interaction amongst subsystems
4) Work done by individual subsystem is integrated

◙ ***Major areas of computer-based applications are:***

1) Finance and accounting
2) Marketing and sales
3) Production
4) Inventory management
5) Human resource management

2. Types of Information System

Operational Level Systems	Knowledge Level Systems	Management Level Systems	Strategic Level Systems	Specialized Systems
1. Transaction Processing Systems (TPS)	1. Office Automation Systems (OAS) 2. Knowledge Management Systems (KMS)	1. Management Information System (MIS) 2. Decision Support System (DSS)	1. Executive Information Systems (EIS)	1. Expert System 2. Cross Functional Information Systems (e.g. ERP) 3. Core Banking System (CBS)

◙ ***Transaction Processing System (TPS):***

- Implemented at operational level
- Process routine business transactions
- Base for higher level systems
- Rapidly process transactions
- Batch processing or on-line processing

Generally TPS involves the following activities:

(i) Punching the transaction
(ii) Processing of transaction
(iii) Generating reports
(iv) Answering queries

TPS Components:

(i) Inputs
(ii) Processing
(iii) Storage
(iv) Output

Features of TPS:

(i) Large volume of data
(ii) Automation of basic operations
(iii) Benefits are easily measurable
(iv) Source of input for other systems

◙ Office Automation Systems

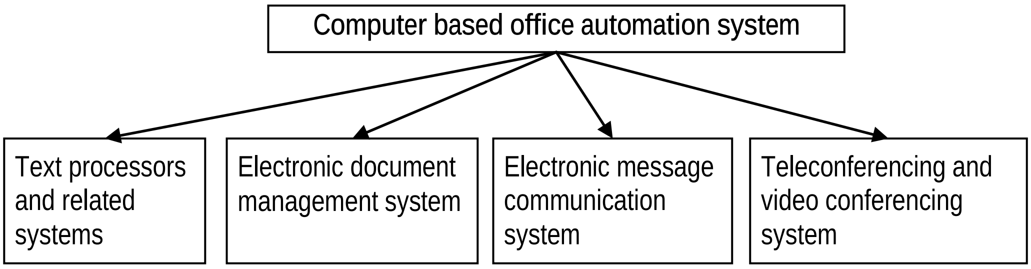
1) Text Processing Systems (TPS)
2) Electronic Document Management System (EDMS)
3) Electronic Message Communication System (EMCS)
4) Teleconferencing and Video Conferencing Systems (TVCS)

Different office activities can be broadly grouped into the following types of operations:

(i) *Document Capture*
(ii) *Document Creation*
(iii) *Receipts and Distribution*
(iv) *Filling, Search, Retrieval and Follow up*
(v) *Calculations*
(vi) *Recording Utilization of Resources*

Benefits of Office Automation Systems:

(i) *Improves communication*
(ii) *Reduces time*
(iii) *Reduces cost*
(iv) *Increases accuracy*


Computer based office automation system
Text processors and related systems
Electronic document management system
Electronic message communication system
Teleconferencing and video conferencing system

I. Text Processing Systems:

- Widely used office system
- Automate the process of development of documents
- Use of standard stored information to produce personalized documents.
- Support laser printers, inkjet printers, scanners
- Example - MS Word.