

Concepts of Governance and Management of Information Systems

[Exam importance- 17 marks; cash topic; only procedural; not technical; easiest chapter of ISCA]

➤ Risk Management:

- Characteristics of Risks:
 1. Potential loss that could occur, if threat materializes
 2. Uncertainty of loss expressed in terms of probability of loss
 3. Probability of threat mounting specific attack against a particular system
- Related Terms: (draw the diagram in JC Book 1.15)
 - Risk: is the likelihood that a threat would exploit the vulnerability in the system and compromise the system in its CIA.
 - Asset: which carries some value to the org. (Char- value; can't be replaced without incurring cost; corporate identity; info classification into 5 types)
 - Vulnerability: weakness in the system security which exposes the system to threats.
 - Threat: Event or action which has a POTENTIAL to cause harm to the system by compromising its CIA.
 - Exposure: Extent of Loss which the org will face when a risk materializes. (estimated cost of loss)
 - Likelihood: Probability that the threat will succeed in achieving its undesirable event.
 - Attack: Set of actions designed to overcome CIA of an information system.
 - Risk: Potential harm to a system if a particular threat materializes and risk analysis means the process of identifying risks to a system and determining their impact on an organization. Risk assessment steps include- Identification; Assessment; Mitigation.
 - Countermeasures: An action, technique or any other measures that reduces the vulnerability of a system.
 - Residual Risk: Any risk still remaining after the counter measures are analyzed and implemented.
- Risk Management Strategies:
 1. Terminate (Eliminate the risk)
 2. Treat (Mitigate the risk)
 3. Transfer (Share the risk)
 4. Tolerate (Accept the risk)
 5. Turn Back (Ignore it :D)
- Key Governance Practices of Risk Management:
 1. Evaluate Risk Mgt.
 2. Direct Risk Mgt.
 3. Monitor Risk Mgt.
- Key Management Practices (processes) of Risk Management:
 1. Collect Data
 2. Analyze Risk
 3. Maintain a Risk Profile
 4. Articulate Risk
 5. Define a Risk Management Action Portfolio
 6. Respond to Risk
- Metrics of Risk Management: (metrics are for measurement)

1. Percentage of critical business processes, IT services, etc. covered by risk assessment
2. Number of significant IT-related incidents that were not identified in risk assessment
3. Percentage of enterprise risk assessments included in IT-related risks
4. Frequency of updating the risk profile based on assessment of risks

➤ Objectives of ISCA and the Role of CA in ISCA:

1. To **understand the key concepts of governance**, risk and compliance aspects relevant to IT in an enterprise
2. To **identify and review IT risks and controls** and risk mgt. approach
3. To **assess BCPlans of Enterprise** from perspective of going concern
4. To **assess SDLC process**
5. To **understand how to perform audit** including collecting and evaluating evidence in an IT environment
6. To **assess the impact** on organizational structure due to **integration of latest technology**
7. To **understand and apply** best practices along with impact of **emerging technologies**

➤ Key Concepts of Governance:

- Governance
- Enterprise Governance
- Corporate Governance (Conformance)
- Business Governance (Performance)

➤ Information Technology and Governance:

- Implementing IT governance as a subset of enterprise governance ensures that implementation of IT meets all the stakeholder requirements including regulators and management.
- Benefits of Governance (direction):
 1. Helps to achieve business objectives (applies everywhere)
 2. Helps align IT strategies with Enterprise strategies
 3. Helps define IT behaviour in the enterprise
 4. Helps to integrate desired processes into the enterprise
 5. Helps to overcome organizational structure limitation
 6. Helps to Improve relationship among BOD, Auditors & Stakeholders

➤ Corporate Governance and IT Governance:

- Corporate Governance
- IT Governance: is a system - by which IT activities in the co. – are directed and controlled – to achieve business objectives – and meet stakeholder needs.
 - Overall objective of IT governance is very much similar to corporate governance but with the focus on IT.

➤ Corporate Governance, ERM and Internal Controls:

- Best practices to Implement corporate governance: (to stop frauds)
 1. Clear assignment of Responsibilities
 2. Establishing mechanism for interaction among BOD, senior mgt. and the auditors
 3. Implementing strong internal control systems
 4. Special monitoring of risk exposures
 5. Financial and managerial incentives to senior mgt. & employees (recognition)
 6. Appropriate information flows; internally and to the public
- Enterprise Risk Management (ERM): is a process, effected by the BOD and applied across the enterprise to identify potential events that may affect the entity, and to manage risk within its risk appetite and also to provide assurance regarding the achievement of entity's objectives.
- Internal Controls:

- ❖ What company should report in its Annual Report against Internal Control Report of Management?
 1. A Statement of Mgt.'s Responsibility for establishing & maintaining adequate internal control over financial reporting for the co.
 2. Framework used by the mgt. for evaluation of the effectiveness of the internal controls
 3. Mgt.'s assessment of the effectiveness of the co.'s internal controls; and disclose material weaknesses, if any
 4. A Statement that Audit firm has issued an attestation report on mgt.'s assessment

- ❖ Internal Controls as per COSO (Committee of Sponsoring Organization): Acc. to COSO, Internal control is comprised of 5 interrelated components:
 1. **Control Environment**- for categorizing the criticality and materiality of each business process
 2. **Risk Assessment**- assess risks associated with each business process
 3. **Control Activities**- to manage, mitigate or reduce risks associated with business process
 4. **Information & Communication**- enable org. to capture & exchange info. for its business processes
 5. **Monitoring**- internal control process must be continuously monitored and modified as required

- Role of IT in Enterprise:
 - Key Functions of IT Steering Committee:
 1. Ensure plans of IT dept. are in tune with enterprise objectives
 2. Review & approve major IT deployment projects
 3. Make decision on all key IT deployments and implementation
 4. Monitor key projects by measuring results of IT projects & its ROI
 5. Review the status of IS Budgets
 6. Review & approve Standards, Policies & Procedures
 7. Facilitate implementation of IT Security within the enterprise
 8. Ensure viable communication system b/w IT and its users
 9. Report to BOD on IT activities on a regular basis

- IT Strategy Planning:
 - 3 levels of managerial activity in an enterprise:
 1. Strategic Planning: following categories:
 - a. Enterprise Strategic Plan (provides over all description under which all units in the enterprise must operate)
 - b. IS Strategic Plan: enablers of IS strategic plan:
 - i. Enterprise business strategy
 - ii. Top management support and involvement
 - iii. Definition of how IT supports the business objectives
 - iv. Inventory of technological solutions & current infra.
 - v. Existing systems assessment
 - vi. Enterprise position on risk & quality
 - c. IS Requirements Plan (defines IS architecture for IS dept.)
 - d. IS Application and Facilities Plan (acq./ dev. schedule; facilities required, etc.)
 2. Management Control
 3. Operational Control
 - Key Mgt. Practices for Aligning IT Strategy with Enterprise Strategy:
 1. Understand enterprise direction
 2. Assess the current env., capabilities and performance
 3. Define the target IT capabilities
 4. Conduct gap analysis
 5. Define the strategic plan and road map

6. Communicate the IT strategy and direction

- Business Value from use of IT (Cost Benefit Analysis): Practices used by mgt. to evaluate whether business value is being derived from use of IT:
 1. Evaluate value optimization (evaluate portfolio of IT-enabled investments; and assess the likelihood of achieving enterprise objectives at reasonable cost)
 2. Direct value optimization (value mgt. principles to derive optimum value throughout the life cycle of IT-enabled inv.)
 3. Monitor value optimization (monitor key goals and benchmarks; and take corrective actions)

Key metrics for the above evaluation:

1. % of IT-enabled investments where benefit realization can be monitored
2. % of IT services and whether expected benefits are realized
3. % of IT-enabled investments and whether claimed benefits are met
4. % of investment with clearly defined expected IT-related costs & benefits
5. % of IT services with clearly defined operational costs and expected benefits
6. Satisfaction survey of stakeholders regarding transparency and their understanding

➤ COBIT 5 – a GEIT Framework:

- Need/ Benefits for Enterprise to use COBIT 5:
 1. Increased value creation from use of IT
 2. Reduced IT-related risks and compliance with laws
 3. Development of business focused IT solutions
 4. Increased enterprise-wide involvement in IT-related activities
- Components in COBIT:
 1. Framework (it helps to organize IT governance objectives and links them to business requirements)
 2. Process descriptions (it provides performance process model in a common language for everyone in the org.)
 3. Control objectives (COBIT defines high level control requirements for each IT process)
 4. Management guidelines (It helps to assign responsibility, performance measurement and relationship b/w process)
 5. Maturity models (It assesses maturity and helps to address gaps)
- Benefits of COBIT 5:
 1. Enables enterprise in achieving their objectives for the governance and mgt. of enterprise IT
 2. Enables IT to be governed and managed in a holistic manner, taking in the full end-to-end business
 3. Helps enterprise to manage IT related risk and ensures CIA
 4. Generic framework- useful for enterprises of all sizes and types
 5. Supports compliance with relevant laws
- Five Principles of COBIT 5:
 - Principle 1: Meeting Stakeholder Needs (create value for them by maintaining balance b/w the risks and benefits; translate their needs into actionable enterprise plans)
 - Principle 2: Covering the enterprise End-to-End (covers all functions and processes within the enterprise and does not just focus on IT function; covers everything and everyone, internal & external which is relevant to the enterprise)
 - Principle 3: Applying Single & Integrated Framework (covering all standards and best practices; also integrates with other frameworks)
 - Principle 4: Enabling Holistic Approach (as a whole; defines set of enablers to support the implementation of a system for enterprise IT)

Principle 5: Separate Governance (eg. IT Act, 1961) from Management (eg. IT Dept.) (makes clear distinction b/w above)

- 7 Enablers of COBIT:
 1. Principles, policies and framework
 2. Processes
 3. Organizational structures
 4. Culture, ethics & behaviour of individuals
 5. Information is pervasive throughout the organizational
 6. Services, infrastructure and applications
 7. People, skills and competencies
- Metrics for measuring successful implementation of GRC in an enterprise:
 1. Reduction of Redundant controls
 2. Reduction in control failures in all key areas
 3. Reduction of expenditure relating to legal & regulatory areas
 4. Improvement through streamlining of processes
 5. Reduction in time through automation of control & compliance measures
 6. Improvement in timely reporting of issues
 7. Dashboard of overall compliance status & key issues to mgt. on real time basis