Chapter - 1

Concepts of Governance and Management of Information Systems

Governance: A **Governance** system typically refers to all the means and mechanisms that will enable multiple stakeholders in an enterprise to have an organized mechanism for evaluating options, setting direction and monitoring compliance and performance, in order to satisfy specific enterprise objectives.

Enterprise Governance: Enterprise Governance can be defined as the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly.
Enterprise Governance has two dimensions:

1. **Corporate Governance or Conformance: Corporate Governance** is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance. The conformance dimension of governance provides a historic view and focuses on regulatory requirements
2. **Business Governance or Performance:** The performance dimension of governance is pro-active in its approach. It is business oriented and takes a forward looking view. This dimension focuses on strategy and value creation with the objective of helping the board to make strategic decisions, understand its risk appetite and its key performance drivers.

1.3.1 Benefits of Governance

Before we proceed further, let us understand the major benefits of governance. These can be summarized as follows:

- Achieving enterprise objectives by ensuring that each element of the mission and strategy are assigned and managed with a clearly understood and transparent decisions rights and accountability framework;
- Defining and encouraging desirable behavior in the use of IT and in the execution of IT outsourcing arrangements;
- Implementing and integrating the desired business processes into the enterprise;
- Providing stability and overcoming the limitations of organizational structure;
- Improving customer, business and internal relationships and satisfaction, and reducing internal territorial strife by formally integrating the customers, business units, and external IT providers into a holistic IT governance framework; and

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

Governance of Enterprise IT (GEIT): GEIT is a sub-set of corporate governance and facilitates implementation of a framework of relevant IS control within an enterprise and encompassing all key areas. The primary objectives of GEIT are to analyze and articulate 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

1. It provides a consistent approach integrated and aligned with the enterprises governance approach.
2. It ensures that IT related dimensions are made in line with the enterprises strategies and objectives.
3. It ensures that IT related dimensions are overseen effectively and transparently.
4. It confirms compliance with legal and regulatory requirements.
5. It ensures that the governance requirements for board members are met.

Key Governance Practices of GEIT: The key governance practices of GEIT are –

1. Evaluate the Governance System of Enterprise IT,
2. Direct the Governance System, and
3. Monitor the Governance System.

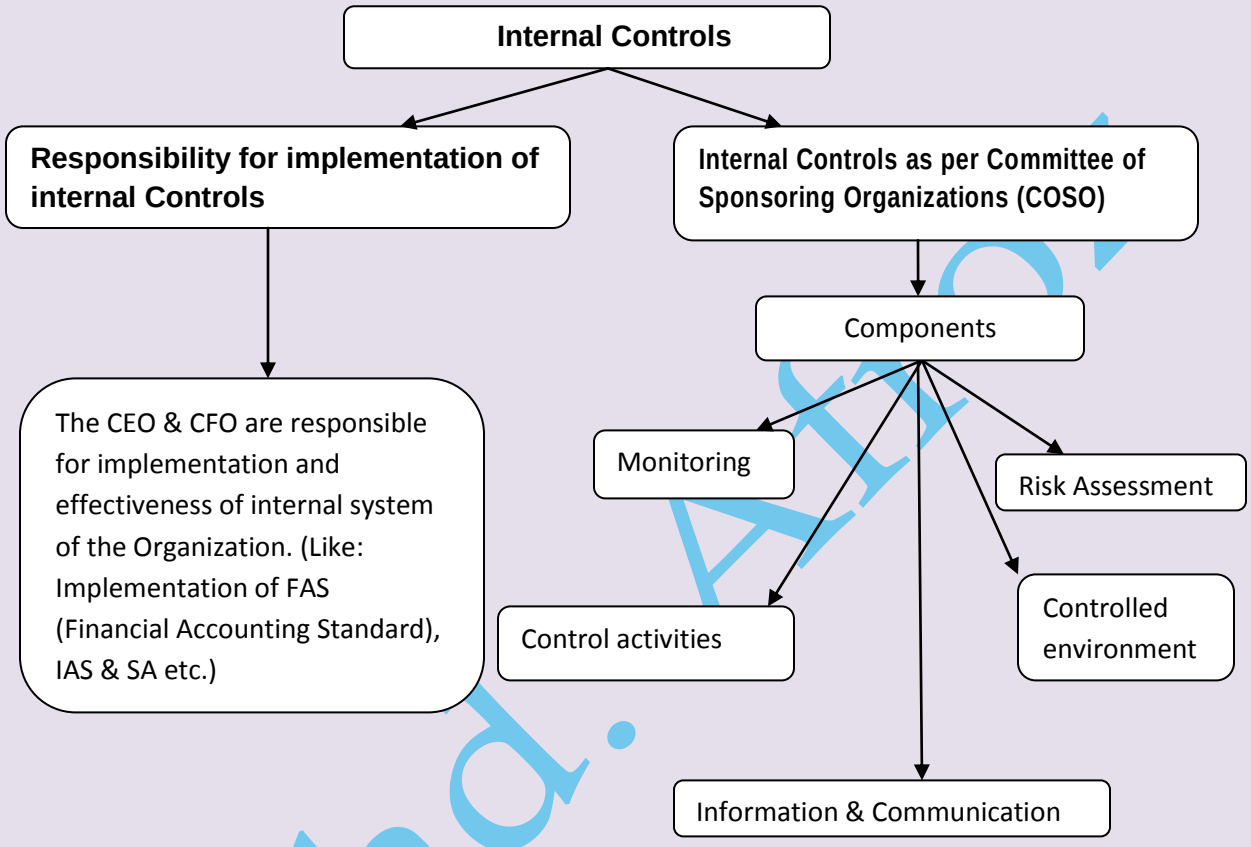
Corporate Governance, Enterprise Risk Management and Internal Controls: Corporate Governance has been defined as the system by which business corporations are directed and controlled. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the Board, managers, shareholders and other stakeholders, and spells out the rules and procedures for making decisions on corporate affairs.

Enterprise Risk Management (ERM) is 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.

The SEC's (The US Security Exchange Commission) final rules define "Internal control over Financial Reporting" as a "process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

1. pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the company;
2. provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles,

3. The receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company;
4. Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements."



Role of IT in Enterprises: It is needless to emphasize that IT is used to perform business processes, activities and tasks and it is important to ensure that IT deployment is oriented towards achievement of business objectives.

IT Steering Committee: Depending on the size and needs of the enterprise, the senior management may appoint a high-level committee to provide appropriate direction to IT deployment and information systems and to ensure that the information technology deployment is in tune with the enterprise business goals and objectives. This committee called as the IT Steering Committee is ideally led by a member of the Board of Directors and comprises of functional heads from all key departments of the enterprise including the audit and IT department.

Key functions of IT Steering Committee: Some of the major function has been mentioned below:

- To ensure that long and short-range plans of the IT department are in tune with enterprise goals and objectives;
- To establish size and scope of IT function and sets priorities within the scope;
- To review and approve major IT deployment projects in all their stages;
- To approve and monitor key projects by measuring result of IT projects in terms of return on investment, etc.;
- To review the status of IS plans and budgets and overall IT performance;
- To review and approve standards, policies and procedures;
- To make decisions on all key aspects of IT deployment and implementation;
- To facilitate implementation of IT security within enterprise;
- To facilitate and resolve conflicts in deployment of IT and ensure availability of a viable communication system exists between IT and its users; and
- 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:

1. **Strategic Planning:** In the context of Information systems, strategic planning refers to the planning undertaken by top management towards meeting long-term objectives of the enterprise.
2. **Management Control:** Management should ensure that IT long and short-range plans are communicated to business process owners and other relevant parties across the enterprise.
3. **Operational Control:** Operational control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Objective of IT Strategy: The primary objective of IT strategy is:

1. To provide a holistic view of the current IT environment,
2. The future direction, and
3. The initiatives required to migrate to the desired future environment (by leveraging enterprise architecture building blocks and components to enable nimble, reliable and efficient response to strategic objectives.)

Classification of strategic Planning: IT Strategy planning in an enterprise could be broadly classified into the following categories:

1. Enterprise Strategic Plan,
2. Information Systems Strategic Plan,
3. Information Systems Requirements Plan, and
4. Information Systems Applications and Facilities Plan.

Key Management Practices for Aligning IT Strategy with Enterprise Strategy: The key management practices, which are required for aligning IT strategy with enterprise strategy are to:

1. Understand enterprise direction,
2. Assess the current environment,
3. Capabilities and performance,
4. Define the target IT capabilities,
5. Conduct a gap analysis,
6. Define the strategic plan and road map and
7. Communicate the IT strategy and direction.

Business Value from use of IT: Business value from use of IT is achieved by ensuring optimization of the value contribution to the business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.

The key management practices: which need to be implemented for evaluating 'whether business value is derived from IT', are highlighted as under:

1. Evaluate Value Optimization,
2. Direct Value Optimization and
3. Monitor Value Optimization

The success of the process of ensuring business value from use of IT can be measured by evaluating the benefits realized from IT enabled investments and services portfolio and the how transparency of IT costs, benefits and risk is implemented. Some of the key metrics, which can be used for such evaluation, are:

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

Risk Management: Risk is the possibility of something adverse happening, resulting in potential loss/exposure. 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.

1.9.2 Sources of Risk

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 as follows:

- Commercial and Legal Relationships,
- Economic Circumstances,
- Human Behavior,
- Natural Events,
- Political Circumstances,
- Technology and Technical Issues,
- Management Activities and Controls, and

Related Terms: Various terminologies relating to risk management are given as follows:

Asset: Asset can be defined as something of value to the organization; e.g., information in electronic or physical form, software systems, employees.
It is the purpose of Information Security Personnel to identify the threats against the assets, the risks and the associated potential damage to, and the safeguarding of Information Assets.

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. A threat is an action, event or condition which ability to inflict harm to the organization resulting in compromise in the system, and/or its quality.

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, loss of reputation, violation of privacy and loss of resources etc.

Likelihood: Likelihood of the threat occurring is the estimation of the probability that the threat will succeed in achieving an undesirable event. The presence, tenacity and strengths of threats, as well as the effectiveness of safeguards must be considered while assessing the likelihood of the threat occurring.

Attack: An attack is an attempt to gain unauthorized access to the system's services or to compromise the system's dependability. In software terms, an attack is a malicious intentional

Risk: Formally, Risk can be defined as the potential harm caused if a particular threat exploits a particular vulnerability to cause damage to an asset.

Risk Analysis is defined as the process of identifying security risks and determining their magnitude and impact on an organization. **Risk assessment** includes the following:

1. Identification of threats and vulnerabilities in the system;
2. Potential impact or magnitude of harm that a loss of CIA, would have on enterprise operations or enterprise assets, should an identified vulnerability be exploited by a threat; and
3. The identification and analysis of security controls for the information system.

Countermeasure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as countermeasure. For example, well known threat 'spoofing the user identity', has two countermeasures:

1. Strong authentication protocols to validate users; and
2. Passwords should not be stored in configuration files instead some secure mechanism should be used.

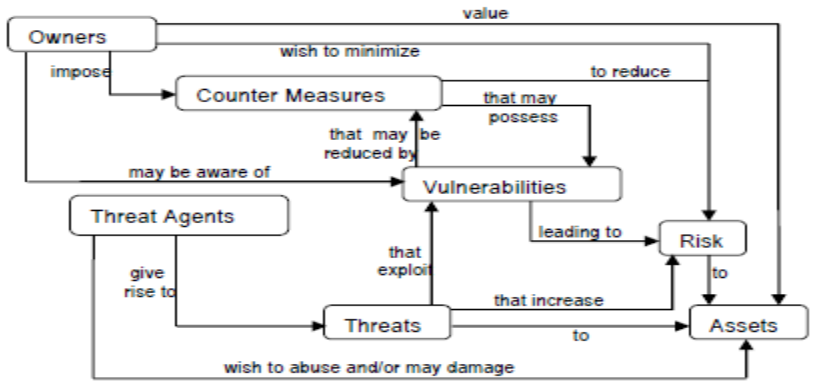


Fig. 1.9.1: Risk and Related Terms*

Risk Management Strategies: Major risk management strategies are

1. Tolerate/Accept the risk,
2. Terminate/Eliminate the risk
3. Transfer/Share the risk,
4. Treat/ mitigate the risk and
5. Turn back.

Key Governance Practices of Risk Management: The key governance practices for evaluating risk management is:

1. To evaluate risk engagement
2. Direct risk management and
3. Monitor risk management.

Key Management Practices of Risk Management: Key Management Practices for implementing Risk Management:

1. Collect Data
2. Analyze Risk
3. Maintain a Risk Profile
4. Articulate Risk
5. Define a Risk Management
6. Action Portfolio and
7. Respond to Risk.

Metrics of Risk Management: Some of the key metrics are as follows:

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

Control Objectives for Information and Related Technology (COBIT)

Control Objectives for Information and Related Technology (COBIT) is a set of best practices for Information Technology management developed by **Information Systems Audit & Control Association (ISACA)** and IT Governance Institute in 1996. ISACA develops and maintains the internationally recognized COBIT framework, helping IT professionals and enterprise leaders fulfill their IT Governance responsibilities while delivering value to the business. The latest ISACA's globally accepted framework COBIT 5 is aimed to provide an end-to-end business view of the governance of enterprise IT that reflects the central role of IT in creating value for enterprises.

COBIT 5 is the only business framework for the governance and management of enterprise Information Technology. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. As per COBIT 5, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but it also raises challenging governance and management issues. This section explains the need for using the approach and latest thinking provided by globally recognized framework COBIT 5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises to simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximize opportunities.

COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy. COBIT 5 enables clear policy development and good practice for IT management.It has following benefits to the Organization:

1. Increased business user satisfaction.
2. Increase value creation from use of IT.
3. Reduce IT related risk and compliance with Law
4. Increase enterprises wide involvement in IT related activities.

The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

Components in COBIT: The components of COBIT are:

1. Framework
2. Process Descriptions
3. Control Objectives
4. Management guidelines and
5. Maturity Model

1.10.4 Benefits of COBIT 5

COBIT 5 frameworks can be implemented in all sizes of enterprises.

- *A comprehensive framework such as COBIT 5 enables enterprises in achieving their objectives for the governance and management of enterprise IT.*
- *The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.*
- *Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT related interests of internal and external stakeholders.*
- *COBIT 5 helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy.*
- *COBIT 5 enables clear policy development and good practice for IT management including increased business user satisfaction.*
- *The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.*
- *COBIT 5 supports compliance with relevant laws, regulations, contractual agreements and policies.*

Principles of COBIT 5

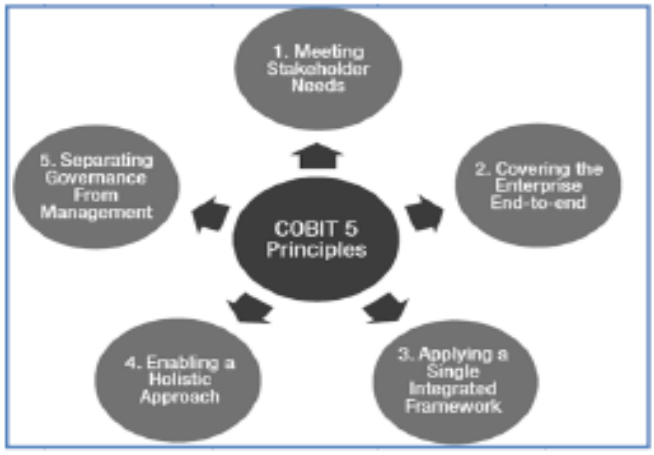


Fig. 1.10.1: Five Principles of COBIT 5*

COBIT 5 Process Reference Model: COBIT 5 includes a Process Reference Model, defines and describes in detail a number of governance and management processes of enterprises. It represents all of the processes found in

an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. **It has two main process domains**: 1. Governance and 2. Management.

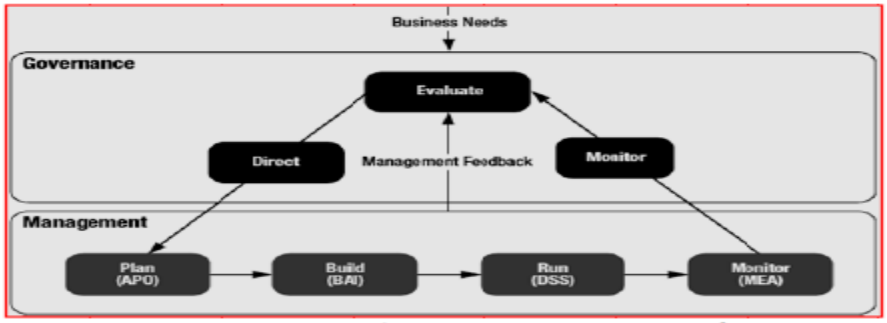


Fig. 1.10.3: Key Areas of Governance and Management*

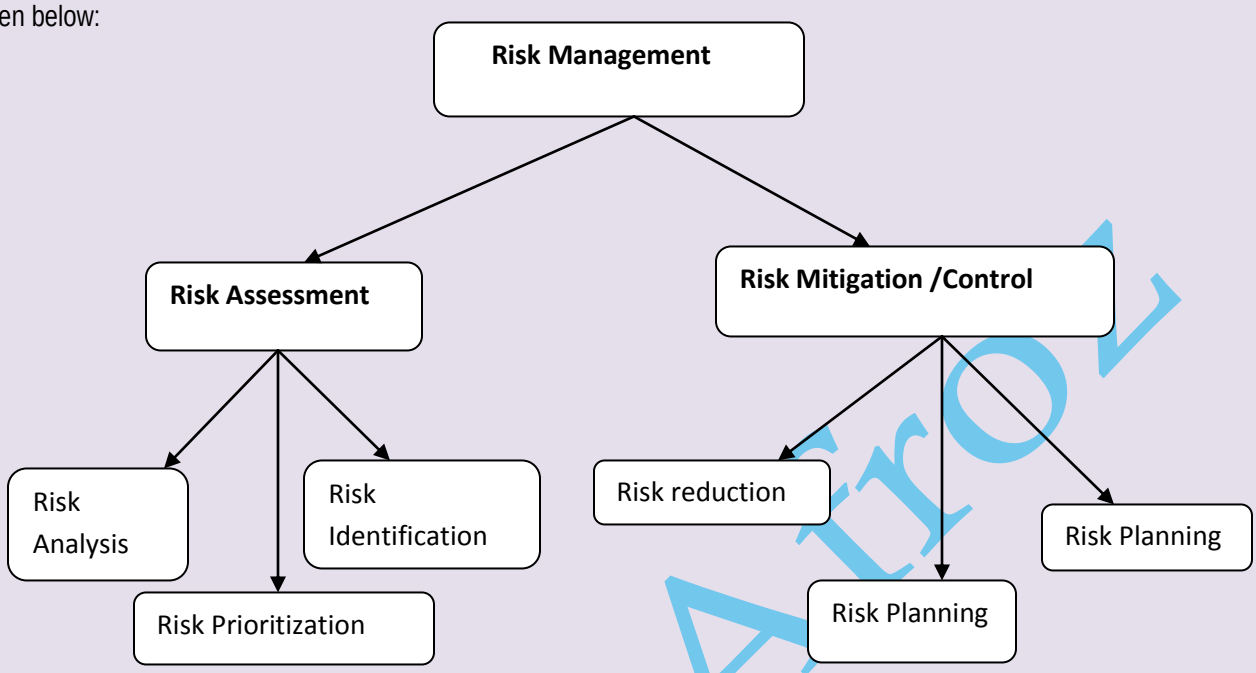
Seven Enablers of COBIT 5: The COBIT 5 framework describes seven categories of enables:

- **Principles, Policies and Frameworks** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
- **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
- **Organizational structures** are the key decision-making entities in an enterprise.
- **Culture, Ethics and Behavior** of individuals and of the enterprise is very often underestimated as a success factor in governance and management activities.

Fig. 1.10.4: Seven Enablers of COBIT 5*

- **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
- **Services, Infrastructure and Applications** include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
- **People, Skills and Competencies** are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.

Risk Management in COBIT 5: A pictorial representation of various activities relating to risk management is given below:



Key Management Practices of IT Compliance: COBIT 5 provides key management practices for ensuring compliance with external compliances as relevant to the enterprise. The practices are:

1. Identify External Compliance Requirements
2. Optimize Response to External Requirements
3. Conform External Compliance and
4. Obtain assurance of external compliance

Using COBIT 5 for information System Assurance: with the help of following Diagram we can better understand the need of COBIT 5 for information System Assurance:

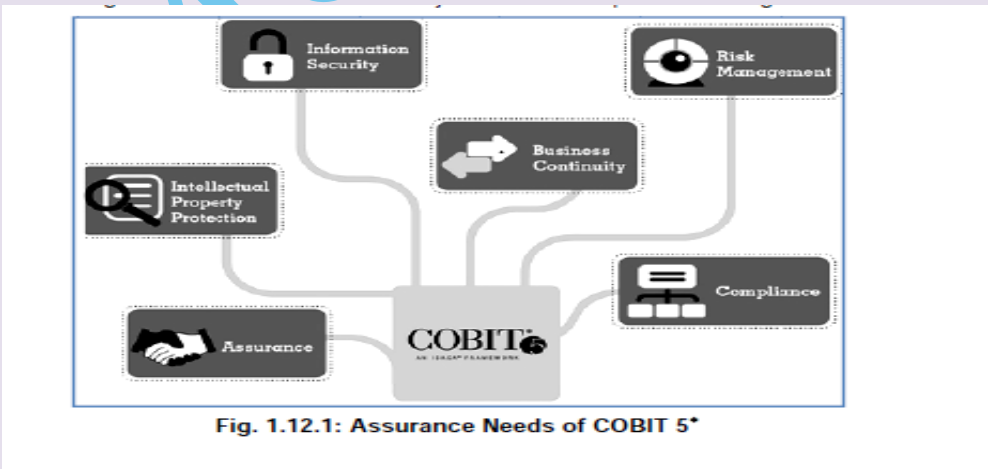


Fig. 1.12.1: Assurance Needs of COBIT 5*

Sample Areas of GRC for Review by Internal Auditors: Major areas, which can be reviewed by internal

auditors as part of review of Governance, Risk and Compliance, are given as follows:

1. Scope
2. Governance
3. Evaluate Enterprise Ethics
4. Risk Management
5. Interpretation
6. Risk Management Process
7. Evaluate Risk Exposures
8. Evaluate Fraud and Fraud Risk
9. Address Adequacy of Risk Management Process

Sample Areas of Review of Assessing and Managing Risks: This review broadly considers whether the enterprise is engaging itself in IT risk-identification and impact analysis, involving multi-disciplinary functions and taking cost-effective measures to mitigate risks. The specific areas evaluated are:

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

Evaluating and Assessing the System of Internal Controls: The key management practices for assessing and evaluating the system of internal controls in an enterprise are:

1. Monitor Internal Controls,
2. Review Business Process Controls Effectiveness,
3. Perform Control Self-assessments,
4. Identify and Report Control Deficiencies,
5. Ensure that assurance providers are independent and qualified,
6. Plan Assurance Initiatives,
7. Scope assurance initiatives and
8. Execute assurance initiatives