Concepts of Governance and Management of Information Systems

Key Concepts of Governance

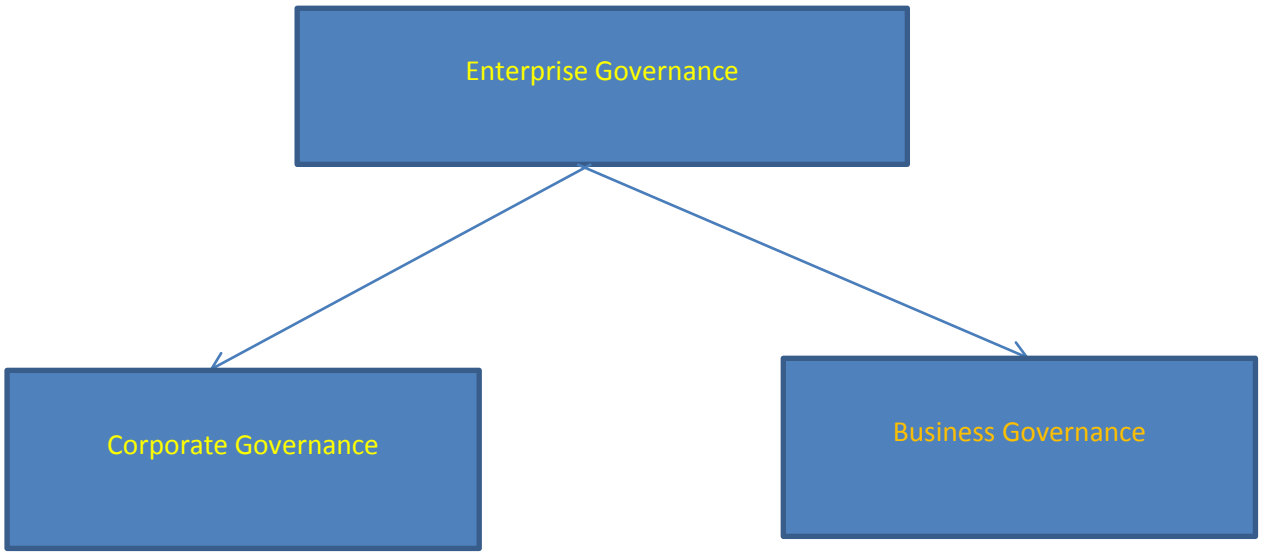
- Organisations exists to deliver value to the stakeholders which is achieved by operating within value and risk parameters

Governance

- Refers to the Means and mechanism
    - Enabling the Multiple stakeholders to
        - Evaluate options
        - Setting direction
        - Monitoring compliance and performance

Enterprise Governance

- Set of responsibilities and practices
- Exercised by the board
- Goal of Providing strategic direction
- Two dimensions



Corporate Governance

- System by which
    - The Company or enterprise is directed and controlled
    - To achieve the objective of increasing shareholder value
- Good corporate governance requires sound internal control procedures
    - Segregation of duties
    - Eliminate conflict of interest

    - Establishing regulators
    - Compliance with rules and regulations
- Good corporate Governance is essential to address
    - Weakness in internal control
    - Stakeholder requirements to be met

Business Governance

- Focuses on the value creation
- Helping the board to take strategic decisions

Information Technology and Governance

- Use of Information Technology in the Key Business Processes has increased through the years
- Regulators have also imposed more Governance Practices in place
- Use of Information Technology in Governance
    - How information is processed
    - How the information is used for the strategic and competitive advantage

Benefits of Governance

- Achieving enterprise objectives by ensuring
    - Mission and strategy are achieved
- Define and encouraging desirable behaviour in use and execution of IT
- Implementing and Integrating the desired Business Processes
- Providing the Stability and overcoming the limitations of organisational structure
- Improving Customer business and internal relationships through
    - Integrating customers, business units
- Enabling effective and strategically aligned decision making

Corporate Governance and IT Governance

- IT Governance is the system by which IT activities in a company or enterprise are directed and controlled to
    - Achieve Business Objectives with objective of
        - Meeting Customer Needs

IT Governance and Governance of Enterprise IT (GEIT)

IT Governance

- It refers to the system in which the
    - Directors of the enterprise
        - evaluate, direct and monitor IT Management to ensure effectiveness, accountability and compliance of IT

Governance of Enterprise IT

- Subset of Corporate Governance which
    - Facilitates implementation of a framework of IS Controls within an enterprise as relevant and encompassing all key areas
- Primary objective of GEIT is
    - Analyse and to make clear the requirements for the governance of enterprise IT

Benefits of Enterprise IT

- Provides an approach aligned with enterprise governance approach
- IT related decisions are made in line with enterprise objects
- IT related processes are overseen effectively and transparently
- Compliance with the legal and regulatory requirements
- Governance requirements of Board of Directors are met

Key Governance Practices of GEIT

- Evaluate the Governance System:- Deal with the stakeholders and make judgement on current and future design of governance of enterprise IT
- Direct the Governance System:- Inform leadership and obtain their support
- Monitor the Governance System:- Monitor the effectiveness and performance of the enterprise's Governance of IT

Corporate Governance

- It refers to the system by which the business corporations are directed and controlled
- Best Practices of Corporate Governance are as follows:-
    - Clear assignment of responsibilities
    - Establishment of hierarchy for the interaction and co-operation
    - Implementing strong internal control systems
    - Special monitoring of risk exposure
    - Financial and Management incentives
    - Appropriate information flows internally and to the public.

Internal Controls

- Process designed by or under the control of the executives of the company
- To be effected by the company's board of directors
- To provide reasonable assurance that the financial reporting and preparation of financial statements are reliable

Responsibility for implementing Internal Controls

- SOX act made the Chief Executive Officers (CEO) and the Chief Financial Officers (CFO) liable for the quality and effectiveness of the organisations internal controls

Internal Controls as per COSO

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative to combat corporate fraud.
- It was established in the United States by five private sector organizations, dedicated to guide executive management and governance entities on relevant aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting.
- COSO is supported by five supporting organizations, including the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International(FEI).

Internal Control is comprised of the five interrelated components as per COSO

- Control Environment: - Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.
- Risk Assessment:- Every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is a prerequisite for determining how the risks should be managed.
- Control Activities:- Control activities are the policies and procedures that help ensure management directives are carried out. Control activities occur throughout the organization, at all levels and in all functions
- Information and Communication:- Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information, that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization.
- Monitoring: - Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time.

  Clause 49 of the Listing agreements issued by SEBI –mandates the implementation of Enterprise Risk Management and Internal controls and holds the senior management responsible for the same

Role of IT in Enterprises

- Enterprises are using Information Technology not only for the Data processing but also for the purpose of Management Information

- IT has not only automated the business processes but also transformed the way the business processes are carried out
- Senior Management has to consider IT as not only an information processing tool but also a tool for better and innovative services

Business and IT Strategy

- There has to be fusion of Information Technology with Business Strategy
- Every Business needs to have the internal control system built into it so that the day to day operations are delivered effectively

IT Steering Committee

An IT Steering Committee is an administrative body that reviews, monitors and prioritizes major IT projects from a cross-functional perspective. The two key concerns of a technology steering committee are:

- **Alignment.** The committee helps ensure that IT strategy is aligned with the strategic goals of the organization.
- **Ownership.** The business units represented on the steering committee have ultimate ownership over the larger IT strategic decisions since those decisions will impact their processes.

- The role and responsibilities of the IT Steering Committee and its members is to be documented and approved by the senior management

- IT Steering Committee is normally headed by a member from the Board of Directors and also functional heads of Key Department personnel

- Key functions of IT Steering Committee are as follows:-

    - Ensuring the long and short range plans of the IT Department are in tune with enterprise goal and objects
    - To review and approve major IT deployment projects in all their stages
    - To review the status of the IS Plans and Budgets and overall IT Performance
    - To review and approve the standards, policies and procedures
    - To report to the Board of Directors on IT activities on a regular basis
    - To approve and monitor key projects by measuring results of IT Projects in terms of Return on Investment

IT Strategy Planning

- There are three levels of Management Activity in an enterprise

  - Strategy Planning:- Deciding on the objectives of the enterprise, on changes in the objectives, on the resources used to attain the objectives, and on the policies to govern the acquisition, use and disposal of resources
  - Management Control:- Process by which managers assure that resources are obtained and used effectively
  - Operational Control:- Process of assuring that the specific tasks are carried out effectively and efficiently

IT Strategic Planning Process

- Management to develop a policy requiring that the Long and Short range plans of the organisation are achieved

Objective of IT Strategy

- Objective is to provide future direction to the organisation, and initiatives required to migrate to desired future environment

Classification of Strategic Planning

- Strategic Planning refers to the planning undertaken by the top management towards meeting long term objectives of the enterprise
- IT Strategic Planning could be classified into the following categories
  - Enterprise Strategic Plan:-
  - Information Systems Strategic Plan
  - Information Systems Requirements Plan
  - Information Systems Applications and Facilities Plan
- Enterprise Strategic Plan:- determines the overall plan of the enterprise, provides the charter in which all units in the organisation must operate. It includes a statement of mission, specification of strategic objectives and assessment of factors affecting the attainment of objectives
- Information Systems Strategic Plan:- The Information System Strategic Plan has to ensure that there is a balance between the IT opportunities and IT business requirement. Some of the enablers of the IS Strategic Plan are:-
  - Enterprise Business Strategy
  - Inventory of technological solutions and current IT infrastructure
  - Monitoring the technological markets
  - Existing System assessments
  - Timely feasibility studies and reality checks
- Information Systems requirements plan:- Enterprise to have clearly defined information architecture with the objective of optimisation of the information systems. Key enablers of the information architecture are as follows:-
  - Automated Data repository and dictionary
  - Data Syntax rules- (set of rules that define combination of symbols)
  - Data ownership and criticality classification

    - Information model representing the business
- Information Systems Applications and Facilities Plan:- On the basis of the information systems architecture and its associated priorities, information systems management can develop an information system and facilities plan. This Plan includes
    - Application systems to be developed
    - Hardware and Software acquisition or development schedule
    - Facilities required and
    - Organisational changes required
- Senior Management is responsible for developing and implementing the long and short range plans that enable the achievement of the enterprise mission and goals

Key Management Practices for Aligning IT strategy with Enterprise Strategy

- **Understand enterprise direction**:-Considering the current enterprise environment and business Processes and also external environment
- **Assess the current environment, capabilities and performance**:-Performance of current internal businesses and IT capabilities and external IT services
- **Define the target IT capabilities**:-Based on understanding the environment and requirements, define the target business and IT capabilities and required IT services
- **Conduct a gap analysis**:-Identify the gap between current and the target environments and consider the alignment of the assets with business outcomes to optimise the investment
- **Define strategic plan and roadmap**:- How the IT related goals will contribute to the enterprise strategic goals
- **Communicate the IT Strategy and direction**:- Communicate to the stakeholders and users throughout the enterprise – the business and IT objectives and direction

Business Value from the use of IT

- It can be achieved by ensuring optimization of the value contribution of the businesses from the business processes, IT Services and IT assets resulting from IT enabled investments at an acceptable cost
- Key Management Practices, need to be implemented to evaluate whether the business value is derived from IT are as follows:-
    - **Evaluate Value Optimisation**:-Evaluate the Portfolio of IT enabled investments to determine likelihood of achieving enterprise objectives, delivering value at reasonable cost
    - **Direct Value Optimisation**:- Optimal value realization from IT enabled investments throughout their full economic cycle
    - **Monitor Value Optimisation**:- to determine the extent to which the enterprise is generating the expected value and benefits to the enterprise from IT enabled investments and services.

Key Metrics that can be used for evaluation of benefits realised from IT related investments are:-

- Percentage of IT enabled investments where
  - Benefit realisation monitored through the full economic life cycle
  - Claimed benefits met or exceeded
- Percentage of IT services
  - Where expected benefits realised
  - With clearly defined and approved operational costs and expected benefits
- Percentage of Investment business cases with clearly defined and approved operational costs and expected benefits

Risk Management

- Effective IT Governance will help to ensure close linkage to the enterprise risk management activities
- Risk assessment approach adopted has to consider business impact of IS risk and different types of risks
- Timely and regular communication of status of residual risks to key stakeholders so that appropriate action is taken to manage the IT Risk profile

Information Systems Risk and Risk Management

- Risk-The Possibility of some adverse happening, resulting in loss
- Management of risk involves-assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk
- Risks in IT environment are mitigated by providing appropriate and adequate IS Security

Sources of Risk

- Common sources of risk are:-
  - Commercial and Legal Relationships
  - Economic Circumstances
  - Human Behaviour
  - Natural Events
  - Political Circumstances
  - Technology and Technical Issues
- Characteristics of Risk
  - Loss Potential Exists exist as a result of threat/vulnerabilities
  - Uncertainity of Loss expressed in terms of probability
  - Likelihood of threat agent mounting an attack against a system

Terms

- Asset
  - Defined as something of value to the organisation
  - Characteristics
    - Recognised to be of value to the organisation
    - Not easily replaceable without cost, skill time, resources
    - Form a part of organisations corporate identity
    - Data collection could be confidential
- Vulnerability
  - The weakness in the system safeguards that exposes the system to threats
  - Vulnerability potentially allows a threat to harm or exploit the system
  - Vulnerability must have one condition out of the following
    - To execute commands as another user
    - Access data that is contrary to access restrictions
    - Pose as another entity
    - Conduct a denial of service
  - Eg:- Short passwords-make the automated system vulnerable to password cracking or guessing routines
- Threat
  - Any entity. Circumstance or event with the potential to harm the software system or component through
    - Its unauthorised access
    - Destruction, Modification or
    - Denial of Service
- Exposure
  - It is the extent of loss the enterprise has to face when a risk materialises
- Likelihood
  - It is the estimation of the probability that the threat would succeed in achieving the undesirable event
- Attack
  - It is an attempt to gain unauthorised access to the systems services or to compromise the system dependability
- Risk
  - Assessment of risk involves the following
    - Identification of threats and vulnerabilities in the system
    - Potential impact that a loss of CIA will have on enterprise operations
    - Identification and analysis of security controls for the information system
  - Gap between need to protect systems and the degree of protection applied is caused by
    - Use of technology
    - Interconnectivity of Systems
    - Elimination of distance, time and space constraints

  - Devolution of Management and control
  - External factors like legislative, legal and regulatory requirements

- Counter measure
  - An action. Device, procedur, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure

- Residual Risk
  - Any risk remaining after the counter measures are analysed and implemented is called residual risk

Risk Management Strategies

- **Tolerate/Accept the risk**
  - Minor risk-whose impact and probability of occurrence is low
  - Consciously accept the risk as a cost of doing business is appropriate
- **Terminate/Eliminate the risk**
  - Risk may be associated with use of technology, supplier or vendor
  - Risk could be eliminated by replacement
- **Transfer/Share the risk**
  - Shared with trading partners
  - Outsourcing Infrastructure Management is the common mode
- **Treat/Mitigate the risk**
  - Controls to be devised to prevent the risk from demonstrating itself or minimising the effects
- **Turn Back**
  - Probability/Impact is low, management may decide to ignore the risk

Key Governance Practices of Risk Management

- Evaluate Risk Management
- Direct Risk Management
- Monitor Risk Management

  - Evaluate Risk Management:-
    - Examine the risk on current and future use of IT in enterprise
  - Direct Risk Management:-
    - Assurance that Risk Management Procedures are appropriate to endure that the actual IT risk not exceed the tolerable risk as per Board
  - Monitor Risk Management:-
    - Monitor the key goals and metrics and set parameters for analysing the deviations and taking remedial action

Key Management Practices of Risk Management

- Collect Data
- Analyse Risk
- Maintain a Risk Profile
- Articulate Risk
- Define a Risk Management Action Portfolio
- Respond to Risk

  - Collect Data:-
    - Relevant data for risk identification, analysis and reporting
  - Analyse Risk:-
    - Develop useful information to support risk decisions
  - Maintain a Risk Profile
    - Maintain an inventory of the known risks and also impacts of the same
  - Articulate Risk
    - Information on the current state of IT Related exposures in timely manner to all stakeholders for appropriate response
  - Define a risk management action portfolio
    - Manage opportunities and reduce the risk to the acceptable level
  - Respond to Risk
    - Respond in timely manner with the effective measures

Metrics for Risk Management

- Enterprises to monitor the processes and practices of IT Risk Management by using metrics. Some of the key metrics are as follows
    - Percentage of Critical business processes, IT –Services and IT-enabled business programs
    - Number of significant IT related incidents not identified in risk assessment
    - Percentage of Enterprise Risk assessments including IT Related Risks
    - Frequency of Updating the risk profile

COBIT 5

- COBIT 5 is the business framework for the governance and management of enterprise IT.

- **COBIT** stands for **Control Objectives for Information and Related Technology**

- It is the product of a global task force and development team from ISACA, a non-profit, independent association of more than 140,000 governance, security, risk and assurance professionals in 187 countries.

- Need for enterprises to use COBIT 5

    - Increased value creation from use of IT
    - User satisfaction with IT engagements and services
    - Reduced IT related risks and compliance with laws, regulations and contractual requirements
    - Development of more business focussed IT Solutions
    - Increased environment wide involvement in IT related activities

- Components in COBIT 5
    - Framework
    - Process Description
    - Control Objectives
    - Management Guidelines
    - Maturity Models

        - Framework:-
            - Organise IT Governance objectives and good practices
        - Process Description:-

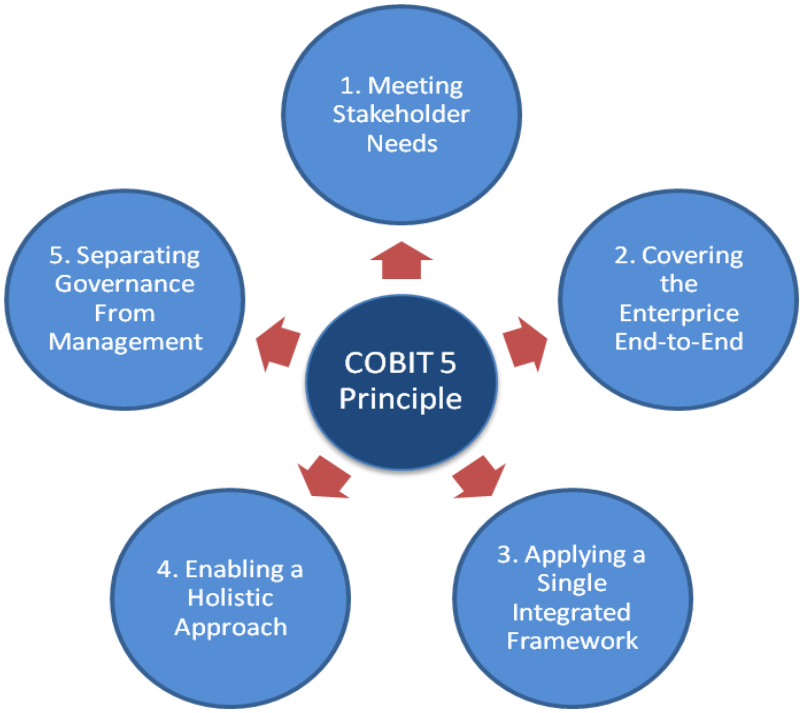
- Reference model and common language for all in an organisation

- Control Objectives
  - Complete set of high level requirements for management consideration
- Management Guidelines
  - Help assign responsibility, agree on objectives, measure performance
- Maturity Models
  - Assess Maturity and Capability per Model

Benefits of COBIT 5

- Achieving Enterprise Objectives- for the governance and management of IT
- Create Optimal Value-through maintaining a balance between realising benefits and optimising risk levels
- Enable Enterprise to be managed in a holistic way
- Manage IT related risks and ensuring compliance, continuity, security and privacy
- Enables clear policy development and good practices for IT Management
- Useful for all enterprises- Commercial or non-profit
- Supports compliance with relevant rules, regulations. Contractual obligations

Principles of COBIT 5



- Meeting Stakeholder Needs:-
  - Enterprises exist to create value for their customers-by maintaining a balance between the realisation of benefits and the optimization of risk and use of resources
  - COBIT 5 provides all the required processes and enablers to support business value creation through the use of IT

- Covering the Enterprise end to end :-
  - COBIT 5 integrates governance of Enterprise IT into enterprise governance-covering all functions and processes within the enterprise
  - COBIT 5 treats the Information and related technologies as assets

- Applying a single integrated framework :-
  - COBIT 5 aligns with other relevant standards and frameworks
  - As such it is complete in enterprise coverage

- Enabling a Holistic Approach
  - Taking into account several interacting components
  - COBIT 5 defines set of enablers to support implementation of a comprehensive governance and management system

- Separating Governance from Management
  - These two require different organisational structures and serve different purposes
  - COBIT 5 framework distinguishes between governance and management

COBIT 5 Enabler Model

- Enabler model includes a total of 37 governance and management processes as mentioned below:-
  - Governance Processes
    - Evaluate Direct and Monitor Practices -5 Processes
  - Management Processes
    - Align, Plan and Organise -13 Processes
    - Build, Acquire and Implement-10 Processes
    - Deliver, Service and Support-6 Processes
    - Monitor, Evaluate and Assess- 3 Processes

Enablers of COBIT 5

- Principles, Policies and Frameworks
- Processes

- Organisational Structures
- Culture, Ethics and Behaviour
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

    - Principles, Policies and Frameworks :-
        - to translate desired behaviour for day to day management
    - Processes:-
        - To achieve certain objectives and produce set of output in achieving overall IT Related goals
    - Organisational Structures:-
        - Key decision making entities in an enterprise
    - Culture, ethics and behaviour:-
        - Often underestimated as a success factor in governance
    - Information:-
        - Pervasive throughout the enterprise
        - Includes all information produced and used by enterprise
    - Services, Infrastructure and Applications
        - Includes the infrastructure, technology and applications
        - Providing the enterprise with information technology processing and services
    - People, Skills and Competencies
        - Linked to people and are required for successful completion of all activities and for making correct decisions

Using COBIT 5 Best Practices for GRC

- **GRC programme implementation** requires the following
    - Define clearly what GRC requirements are applicable
    - Identifying the regulatory and compliance landscape
    - Reviewing the current GRC status
    - Determining most optimal approach
    - Setting out key parameters on which success will be measured
    - Using a process oriented approach

- **Success of GRC can be measured** by using the following goals and metrics
    - **Reduction**
        - Of redundant controls and time to execute
        - In control failures

        - Of expenditure relating to legal, regulatory and review areas
        - In overall time required for audit for key business areas
    - **Improvement**
        - through the streamlining of processes and reduction in time through automation of control and compliance procedures
        - In timely reporting of regular compliance issues and remediation measures

IT Compliance Review

- Effective implementation of ERM requires consideration of multiple factors such as
    - Using a holistic approach
    - Covering enterprise end to end
    - Top Down approach
    - Best Practices Framework
    - Technology Deployment
    - Related Regulatory requirements
    - Business Needs

Key Management Practices of IT Compliance

- COBIT 5 provides Key Management Practices for ensuring compliance with the external compliances as relevant to the enterprise
- The Key Management Practices are:-
    - Identify External Compliance Requirements
    - Optimise Response to External Requirements
    - Confirm External Compliance
    - Obtain Assurance of External Compliance

        - **Identify External Compliance** Requirements:-
            - Identify the changes in local and international laws, regulations and other external requirements
        - **Optimise Response** to External Requirements
            - Review and adjust policies, principles, standards. procedures and methodologies to ensure
                - Legal. Regulatory and contractual requirements are addressed and communicated
        - **Confirm External Compliances**
            - Confirm compliance of policies, principles, standards, procedures and methodologies with legal regulatory and contractual requirements
        - **Obtain Assurance of External Compliance**

- Obtain and Report assurance of Compliance and adherence with policies, principles, standards, procedures and methodologies

Key metrics for Assessing Compliance Process

- **Compliance with External Laws and Regulations**- These metrics are as follows
  - Cost of IT non-Compliance
  - Number of IT related non-compliance issues reported to the board
  - Number of Non-Compliance issues relating to contractual agreements with IT Service Providers
- **Compliance with Internal Policies** :-
  - Number of incidents related to non- compliance of policy
  - Percentage of Stakeholders who understand policies
  - Frequency of Policy review and updates

Evaluating IT Governance Structure and Practices by Internal Auditors

- The Institute of Internal Auditors-Outlines specific areas and critical aspects relating to governance structure and practices which can be reviewed as a part of Internal Audit

  - **Leadership:-**
    - Evaluate relationship between IT objectives and current strategic needs of the organisation
    - Determine how IT will be measured in helping the organisation achieve its goals
    - Review how roles and responsibilities are assigned within the IT organisation
    - Review the role of senior management and board in helping establish and maintain strong IT Governance
  - **Organisational Structure:-**
    - Review interaction of the organisation management and IT Personnel
    - Existence of Roles and Reporting Relationships
  - **Processes**
    - Evaluate IT process activities and controls in place to mitigate the risks to the organisation
    - Processes used by IT organisation to support the IT environment
  - **Risks**
    - Review processes used to identify, monitor and assess risk
    - Determine the Accountability that the Personnel have within risk management

- **Controls**
  - Assess key controls that are defined by IT to manage its activities
  - Ownership, documentation and reporting of self -validation aspects to be reviewed by internal audit
  - Control to be robust enough to address identified issues
- **Performance Measurement/Monitoring**
  - Evaluate the framework and systems in place to measure and monitor organisational outcomes where IT support plays a major role

Sample areas of GRC review by Internal Auditors

- IIA provides the areas, which can be reviewed by Internal Auditors as part of review of GRC
  - Scope
    - Internal Audit to evaluate and contribute to improvement of GRC processes
  - Governance
    - Assess and Make appropriate recommendations for improving Governance process
      - Promote ethics
      - Ensure organisation performance management
      - Communicating risk and control information to appropriate areas
      - Coordinating the activities
  - Evaluate Enterprise ethics
    - Whether IT governance of the organisation supports the organisation strategy and objectives
  - Risk Management
    - Evaluate effectiveness and contribute to improvement
  - Interpretation
    - Risk Management Processes are effective
      - Organisation objectives aligned with the organisation mission
      - Significant risks are identified and assessed
      - Appropriate risk responses are selected
      - Relevant risk information is captured and communicated in timely manner
  - Risk Management Process
    - Monitor through on-going management activities, separate evaluations or both
  - Evaluate Risk Exposures
    - Achievement of Objectives

        - Reliability and Integrity of Financial and Operations Information\
        - Effectiveness and efficiency of Programs
        - Safeguarding of assets
        - Compliance with laws, regulations, policies

    - Evaluate Fraud and Fraud risk
        - Evaluate potential for the occurrence of fraud and how it manages the fraud risk
    - Address Adequacy of Risk Management Process
        - Address risk consistent with organisation objectives and be alert to existence of other risks

Sample areas of review of Assessing and Managing Risks

- This review considers whether the enterprise is engaging itself in the IT Risk identification and impact analysis
- Areas evaluated are
    - Risk Management Ownership and accountability
    - Different kinds of IT Risks
    - Defined and communicated risk tolerance profile
    - Root cause and analyses and risk mitigation measures
    - Risk assessment methodology

Evaluating and assessing the system of Internal Controls

- COBIT 5 has specific process-MEA 02- Monitor, Evaluate and Assess the System of Internal Control-Providing guidance on evaluating and assessing Internal Controls
- Objective of such a review is
    - Continuously monitor and evaluate the control environment
    - Enable Management to identify deficiencies and inefficiencies

Key Management Practices for assessing and evaluating the system of Internal Control

- 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
- Scope assurance initiatives
- Execute assurance initiatives