CHAPTER-1

Concepts of Governance and Management of Information Systems

Giridhar Dande
G's publiCAtions

Key Concepts of Governance

Governance

The term “Governance” is derived from the Greek verb meaning “to steer”.

Governance refers to "all processes of governing, whether undertaken by a government, market or network, whether over a family, tribe, formal or informal organization or territory and whether through laws, norms, power or language."

It relates to "the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions.

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

‘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 is an overarching framework into which many tools and techniques and codes of best practice can fit.

Examples include codes on corporate governance and financial reporting standards.

Enterprise Governance has two dimensions:

1.Corporate Governance or Conformance

2. Business Governance or Performance

Conformance means – another term for conformity

1.Corporate Governance or Conformance

the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.

Corporate governance refers to the structures and processes for the direction and control of companies.

Corporate governance concerns the relationships among the management, Board of Directors, the controlling shareholders and other stakeholders.

The corporate governance provides a historic view and focuses on regulatory requirements.

Good corporate governance contributes to sustainable economic development by enhancing the performance of companies and increasing their access to outside capital.

The Sarbanes Oxley Act of US and the Clause 49 listing requirements of SEBI are examples of providing for such compliances from conformance perspective.

2.Business Governance or Performance

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.

This dimension does not lend itself easily to a regime of standards and assurance as this is specific to enterprise goals and varies based on the mechanism to achieve them.

It is advisable to develop appropriate best practices, tools and techniques such as balanced scorecards and strategic enterprise systems that can be applied intelligently for different types of enterprises as required.

Benefits of Governance

- 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.

- Enabling effective and strategically aligned decision making for the IT Principles that define the

role of IT,
IT Architecture,
IT Infrastructure,
Application Portfolio and Frameworks,
Service Portfolio,
Information and Competency Portfolios and
IT Investment & Prioritization.

IT Governance and Governance of Enterprise IT (GEIT)

IT Governance

Key practices to determine status of IT Governance

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

Benefits of IT Governance

The benefits, which are achieved by improving governance or management of enterprise, IT would depend on the specific and unique environment of every enterprise. At the highest level, these could include:

Increased	- value delivered through IT enterprise. - user satisfaction with IT services
Improved	- agility in supporting business needs - management and mitigation of IT-related business risk - transparency and understanding of IT's contribution to the business.

	- compliance with relevant laws, regulations and policies.
- Better cost performance of IT - IT becoming an enabler for change rather than an inhibitor. - More optimal utilization of IT resources	

Governance of Enterprise IT (GEIT)

Governance of Enterprise IT(GEIT) is a sub-set of corporate governance and facilitates implementation of a framework of IS controls within an enterprise as relevant 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.

Key Governance Practices of GEIT

Evaluate	Direct	Monitor
the Governance System		
Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgment on the current and future design of GEIT.	Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of IT in line with agreed governance design principles, decision-making models and authority levels. Define the information required for informed decision making	Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms are operating effectively and provide appropriate oversight of IT

Benefits of GEIT

It ensures	- that IT-related decisions are made in line with the enterprise's strategies and objectives. - that IT-related processes are overseen effectively and transparently. - that the governance requirements for board members are met.
- It provides a consistent approach integrated and aligned with the enterprise governance approach. - It confirms compliance with legal and regulatory requirements.	

Corporate Governance, Enterprise Risk Management and Internal Controls

Corporate Governance

The concept of Corporate Governance has succeeded in attracting a good deal of public interest because of its importance for the economic health of corporations, protect the interest of stakeholders including investors and the welfare of society, in general.

Some of the best practices of corporate governance include the following:

1. Clear assignment of responsibilities and decision-making authorities, incorporating a hierarchy of required approvals from individuals to the board of directors.

2.Establishment of a mechanism for the interaction and cooperation among the

board of directors,

senior management and
the auditors.

3. Implementing

strong internal control systems, including
internal and external audit functions,
risk management functions independent of business lines, and
other checks and balances.

4. Special monitoring of risk exposures where conflicts of interest are likely to be particularly great,

including business relationships with borrowers affiliated with the bank,
large shareholders,
senior management, or
key decision-makers within the firm.

5. Financial and managerial incentives to act in an appropriate manner offered to senior management, business line management and employees in the form of compensation, promotion and other recognition.

Enterprise Risk Management (ERM)

Enterprise Risk Management deals with risks and opportunities affecting value creation or preservation, defined as follows:

"Enterprise Risk Management is a process, effected 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."

It is important for management to ensure that the enterprise risk management strategy considers implementation of information and its associated risks while formulating IT security and controls as relevant.

IT security and controls are a sub-set of the overall enterprise risk management strategy and encompass all aspects of activities and operations of the enterprise.

Internal Controls

Internal Controls as per COSO

In a computerized environment, the goals of asset safeguarding, data integrity, system efficiency and system effectiveness can be achieved only if an organization's management sets up a system of internal controls.

According to COSO, Internal Control is comprised of five interrelated components: **(I-C-RCM)**

Information and Communication:

These are the elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.

These are associated with control activities regarding information and communication systems of the entity that acts as one of the component of internal accounting system.

These enable an organization to capture and exchange the information needed to conduct, manage, and control its business processes.

Control Environment:

This includes the elements that establish the control context in which specific accounting systems and control procedures must operate.

The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.

For each business process, an organization needs to develop and maintain a control environment including categorizing the criticality and materiality of each business process, plus the owners of the business process.

Risk Assessment:

This includes the elements that identify and analyze the risks faced by an organization and the way the risk can be managed.

Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organization.

A control environment must include an assessment of the risks associated with each business process.

Control Activities:

This includes the elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records.

These are called accounting controls.

Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.

Control activities must be developed to manage, mitigate, and reduce the risks associated with each business process. It is unrealistic to expect to eliminate risks completely.

Monitoring:

The internal control process must be continuously monitored with modifications made as warranted by changing conditions.

This includes the elements that ensure internal controls operate reliably over time.

The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

Role of IT in Enterprises

Implementing IT has to consider not only implementation of IT controls from conformance perspective but also IT could be a key enabler for providing strategic and competitive advantage.

This requires that senior management considers IT not only as an information processing tool but more from a strategic perspective to provide better and innovative services.

This makes it imperative to develop an IT strategy, which is aligned with business strategy and ensures value creation and facilitates benefit realization from the IT investments.

IT Steering Committee

As enterprises are dependent on the information generated by information systems, it is important that planning relating to information systems is undertaken by senior management or by the 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.

The role and responsibility of the IT Steering Committee and its members must be documented and approved by senior management.

The IT Steering Committee provides overall direction to deployment of IT and information systems in the enterprises.

The key functions of the committee would include of the following:

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

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 3 levels of managerial activity in an enterprise:

Level-1 Strategic Planning:

Strategic Planning is defined as the process of deciding on objectives of the enterprise, on changes in these objectives, on the resources used to attain these objectives, and on the policies that are to govern the acquisition, use, and disposition of these resources.

Strategic planning is the process by which top management determines overall organizational purposes and objectives and how they are to be achieved.

Corporate-level strategic planning is the process of determining the overall character and purpose of the organization, the business it will enter and leave, and how resources will be distributed among those businesses.

Level-2 Management Control:

Management Control is defined as the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objectives.

Level-3 Operational Control:

Operational Control is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

Classification of Strategic Planning – 4 types

1. Enterprise Strategic Plan - ESP

Business Planning determines the overall plan of the enterprise.

The enterprise strategic plan provides the overall charter under which all units in the enterprise, including the information systems function must operate.

It is the primary plan prepared by top management of the enterprise that guides the long run development of the enterprise.

It includes a statement of mission, a specification of strategic objectives, an assessment of environmental and organization factors that affect the attainment of these objectives, a statement of strategies for achieving the objectives, a specification of constraints that apply, and a listing of priorities.

In an IT environment, it is important to ensure that the IT plan is aligned with the enterprise plan.

2. Information Systems Strategic Plan - ISSP

The IS strategic plan in an enterprise has to focus on striking an optimum balance of IT opportunities and IT business requirements as well as ensuring its further accomplishment.

This would require the enterprise to have a strategic planning process undertaken at regular intervals giving rise to long -term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

Some of the enablers of the IS Strategic plan are:

Enterprise business strategy,
Definition of how IT supports the business objectives,
Inventory of technological solutions and current infrastructure,
Monitoring the technology markets,
Timely feasibility studies and reality checks,
Existing systems assessments,
Enterprise position on risk,
time-to-market,
quality, and
Need for senior management buy-in,
support and critical review.

3.Information Systems Requirements Plan - ISRP

Every enterprise needs to have clearly defined information architecture with the objective of optimizing the organization of the information systems.

This requires creation and continuous maintenance of a business information model and also ensuring that appropriate systems are defined to optimize the use of this information.

Based on the information architecture requirements of an enterprise, the Information Systems Requirements Plan has to be drawn up so as to meet the information requirements of the enterprise.

Some of the key enablers of the information architecture are as follows:

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

4.Information Systems Applications and Facilities Plan - ISAFP

On the basis of the information systems architecture and its associated priorities, the information systems management can develop an 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.

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 highlighted here:

Understand enterprise direction:

Consider the current enterprise environment and business processes, as well as the enterprise strategy and future objectives.

Consider also the external environment of the enterprise.

Conduct a gap analysis:

Identify the gaps between the current and target environments and consider the alignment of assets with business outcomes to optimize investment in and utilization of the internal and external asset base.

Consider the critical success factors to support strategy execution.

Assess the current environment, capabilities and performance:

Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT.

Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement.

Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.

Communicate the IT strategy and direction:

Create awareness and understanding of the business and IT objectives and direction, as captured in the IT strategy, through communication to appropriate stakeholders and users throughout the enterprise.

Define the strategic plan and road map:

Create a strategic plan that defines, in co- operation with relevant stakeholders, how IT- related goals will contribute to the enterprise's strategic goals.

Include how IT will support

IT-enabled investment programs,
business processes,
IT services and IT assets.

IT should define the initiatives that will be required to close the gaps, the sourcing strategy, and the measurements to be used to monitor achievement of goals, then prioritize the initiatives and combine them in a high- level road map.

Business Value from Use of IT

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

Evaluate	Direct	Monitor
Value Optimization		
Continually evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgment on any changes in direction that need to be given to management to optimize value creation.	Direct value management principles and practices to enable optimal value realization from IT enabled investments throughout their full economic life cycle.	Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.

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. - enabled investments where claimed benefits met or exceeded.
	- services where expected benefits realized. -services with clearly defined and approved operational costs and expected benefits
- Percentage of investment business cases with clearly defined and approved expected IT related costs and benefits.	

- Satisfaction survey of key stakeholders regarding the transparency, understanding and accuracy of IT financial info.

Risk Management

Sources of Risk

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
Individual Activities.

Related Terms

Asset	Vulnerability	Threat
Exposure	Likelihood	Attack
Risk	Counter Measure	

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

Irrespective the nature of the assets themselves, they all have one or more of the **following characteristics:**

1.They are recognized to be of value to the organization.
2.They are not easily replaceable without cost, skill, time, resources or a combination.
3.They form a part of the organization's corporate identity, without which, the organization may be threatened.
4.Their Data Classification would normally be Proprietary, Highly confidential or even Top Secret.

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.

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 automated information 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

unauthorized access,
destruction,

modification,
and/or denial of service is called a Threat.

A threat is an action, event or condition where there is a compromise in the system, its quality and ability to inflict harm to the organization.

Threat has capability to attack on a system with intent to harm and cannot exist without a target asset.

Threats are typically prevented by applying some sort of protection to assets.

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 fault, usually an external fault that has the intent of exploiting vulnerability in the targeted software or system.

Simply, it is the act of trying to defeat Information Systems (IS) safeguards.

The type of attack and its degree of success determines the consequence of the attack.

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, and 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:

-Identification of threats and vulnerabilities in the system;

-Potential impact of harm that a loss of CIA, would have on enterprise operations or assets.

-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 is caused by: (WIDE-UAE)

Widespread use of technology.
Interconnectivity of systems.
Devolution of management and control.
Elimination of distance, time and space as constraints.
Unevenness of technological changes.

Attractiveness of conducting unconventional electronic attacks against organizations.
External factors such as legislative, legal and regulatory requirements or technological developments.

Counter Measure: An action, device, procedure, technique or other measure that reduces the vulnerability of a component or system is referred as Counter Measure.

For example, well known threat 'spoofing the user identity', has two countermeasures:

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

Risk Management Strategies – T[5]

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them.

Some risks may be minor, and it may not be cost effective to implement expensive control processes for them.

Risk management strategy is explained and illustrated below:

Tolerate/Accept the risk

One of the primary functions of management is managing risk.

Some risks may be considered minor because their impact and probability of occurrence is low.

In this case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

Terminate/Eliminate the risk

It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor.

The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

Transfer/Share the risk

Risk mitigation approaches can be shared with trading partners and suppliers.

A good example is outsourcing infrastructure management.

In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization.

Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

Treat/mitigate the risk

Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

Turn back

Where the probability or impact of the risk is very low, then management may decide to ignore the risk.

Key Governance Practices of Risk Management

Evaluate	Direct	Monitor
Risk Management		
Continually examine and make judgment on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risks to enterprise value related to the use of IT are identified and managed;	Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite	Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.

Key Management Practices of Risk Management –(CM-RADA)

Collect Data: Identify and collect relevant data to enable effective IT related risk identification, analysis and reporting.

Maintain a Risk Profile: Maintain an inventory of known risks and risk attributes, including

expected frequency,
potential impact,
responses,
related resources,
capabilities, and
current control activities.

Respond to Risk: Respond in a timely manner with effective measures to limit the magnitude of loss from IT related events.

Analyze Risk: Develop useful information to support risk decisions that take into account the business relevance of risk factors.

Define a Risk Management Action Portfolio: Manage opportunities and reduce risk to an acceptable level as a portfolio.

Articulate Risk: Provide information on the current state of IT- related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.

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.

4.Frequency of updating the risk profile based on status of assessment of risks.

COBIT 5 Business Framework – Governance and Management of Enterprise IT

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.

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.

Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions.

COBIT 5 provides good practices in governance and management to address these critical business issues.

It is a set of globally accepted principles, practices, analytical tools and models that can be customized for enterprises of all sizes, industries and geographies.

It helps enterprises to create optimal value from their information and technology.

It provides the tools necessary to understand, utilize, implement and direct important IT related activities, and make more informed decisions through simplified navigation and use.

COBIT 5 is intended for enterprises of all types and sizes, including non - profit and public sector and is designed to deliver business benefits to enterprises, including:

- **User** satisfaction with IT engagement and services;
- **I**ncreased value creation from use of IT;
- **R**educed IT related risks and compliance with laws, regulations and contractual requirements;
- **D**evelopment of more business-focused IT solutions and services;
- **I**ncreased enterprise wide involvement in IT-related activities.

Integrating COBIT 5 with Other Frameworks

COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance.

COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as

Information Technology Infrastructure Library (**ITIL**),

The Open Group Architecture Framework (**TOGAF**) and

ISO 27001.

Thus, COBIT 5 acts as the single overarching framework, which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language.

Components in COBIT – (M-CMPF)

Management Guidelines

Help assign responsibility, agree on objectives, measure performance, and illustrate interrelationship with other processes.

Control Objectives

Provide a complete set of high-level requirements to be considered by management for effective control of each IT process.

Maturity Models

Assess maturity and capability per process and helps to address gaps.

Process Descriptions

A reference process model and common language for everyone in an organization. The processes map to responsibility areas of plan, build, run and monitor.

Framework

Organize IT governance objectives and good practices by IT domains and processes, and links them to business requirements;

Benefits of COBIT 5

COBIT-5	- enables enterprises in achieving their objectives for the governance and management of enterprise IT. - help enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. - 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. - helps enterprises to manage IT related risk and ensures compliance, continuity, security and privacy. - enables clear policy development and good practice for IT management including increased business user satisfaction. - is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector. - supports compliance with relevant laws, regulations, contractual agreements and policies.

Five Principles of COBIT 5

Principle 1: Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and use of resources.

It provides all of the required processes and other enablers to support business value creation through the use of IT.

Because every enterprise has different objectives, an enterprise can customize COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT related goals and mapping these to specific processes and practices.

Stakeholder needs have to be transformed into an enterprise's actionable strategy.

The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customized enterprise goals, IT related goals and enabler goals.

This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 integrates governance of enterprise IT into enterprise governance.

It covers all functions and processes within the enterprise.

COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise.

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

There are many IT related standards and best practices, each providing guidance on a subset of IT activities.

COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, thus allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator.

It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components.

COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

Enablers are broadly defined as anything that can help to achieve the objectives of the enterprise.

Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between governance and management.

These two disciplines encompass different types of activities, require different organizational structures and serve different purposes.

Seven Enablers of COBIT 5

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.

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.

Using COBIT 5 Best Practices for GRC

GRC program implementation requires the following:

1.Defining clearly what GRC requirements are applicable.
2.Identifying the regulatory and compliance landscape.
3.Reviewing the current GRC status.
4.Determining the most optimal approach.
5.Setting out key parameters on which success will be measured.
6.Using a process oriented approach.
7.Adapting global best practices as applicable.
8.Using uniform and structured approach which is auditable.

GRC program can be measured by using the following goals and metrics:

1.The reduction of redundant controls and related time to execute.

2.The reduction in control failures in all key areas.

3.The reduction of expenditure relating to legal, regulatory and review areas.

4.Reduction in overall time required for audit for key business areas.

5.Improvement through streamlining of processes and reduction in time through automation of control and compliance measures.

6.Improvement in timely reporting of regular compliance issues and remediation measures.

7.Dashboard of overall compliance status and key issues to senior management on a real - time basis as required.

IT Compliance Review

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 given as follows:

Identify External Compliance Requirements

On a continuous basis, identify and monitor for changes in local and international laws, regulations, and other external requirements that must be complied with from an IT perspective.

Optimize Response to External Requirements

Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated.

Consider industry standards,
codes of good practice,
and best practice guidance for adoption and adaptation.

Confirm External Compliance

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.

Confirm that corrective actions to address compliance gaps are closed in a timely manner.

Key Metrics for Assessing Compliance Process

Compliance with External Laws and Regulations	Compliance with Internal Policies
-Cost of IT non-compliance, including settlements and fines. -Number of IT related non-compliance issues reported to the board or causing public comment or embarrassment. -Number of non-compliance issues relating to contractual agreements with IT service providers. -Coverage of compliance assessments.	-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 System Assurance

Using COBIT 5 for Information System Assurance

COBIT 5 has been engineered to meet expectations of multiple stakeholders.

It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc.

It is written in a non -technical language and is therefore, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers, regulators for understanding and addressing IT related issues as relevant to them.

Globally from the GRC perspective, COBIT has been widely used with COSO by management, IT professionals, regulators and auditors (internal/external) for implementing or evaluating Governance and management practices from an end-to-end perspective.

COBIT has been used as an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001 etc. have been integrated into overall enterprise governance.

Evaluating IT Governance Structure and Practices by Internal Auditors

The following guidance is from internal audit perspective as issued by The Institute of Internal Auditors (IIA).

Leadership

- Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel.

- Assess the involvement of IT leadership in the development and on-going execution of the organization's strategic goals.

- Determine how IT will be measured in helping the organization achieve these goals.

- Review how roles and responsibilities are assigned within the IT organization and how they are executed.

- Review the role of senior management and the board in helping establish and maintain strong IT governance.

Organizational Structure

- Review how organization management and IT personnel are interacting and communicating current and future needs across the organization.

- This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization.

Processes

- Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems.

- What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?

Risks

- Review the processes used by the IT organization to identify, assess, and monitor risks within the IT environment.

- Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.

Controls

- Assess key controls that are defined by IT to manage its activities and the support of the overall organization.

- Ownership, documentation, and reporting of self-validation aspects should be reviewed as activity of internal audit.

- Additionally, the control set should be strong enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.

Performance Measurement

- Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

Sample Areas of GRC for Review by Internal Auditors – SEG-RIREEA

Scope: The internal audit activity must evaluate and contribute to the

improvement of governance,
risk management, and
control processes using a systematic and disciplined approach.

Evaluate Enterprise Ethics: The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics related objectives, programs, and activities.

The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

Governance: internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

1.Promoting appropriate ethics and values within the organization.

2.Ensuring effective organizational performance management and accountability.

3.Communicating risk and control information to appropriate areas of the organization.

4.Coordinating the activities of and communicating information among the board, external and internal auditors, and management.

Risk Management: The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Interpretation: Determining whether risk management processes are effective in a judgment resulting from the internal auditor's assessment.

Risk Management Process: The internal audit activity may gather the information to support this assessment during multiple engagements.

The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Evaluate Risk Exposures: The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.

Evaluate Fraud and Fraud Risk: The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Address Adequacy of Risk Management Process: During consulting engagements, internal auditors must address risk consistent with the engagement's objectives and be alert to the existence of other significant risks.

Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

Sample Areas of Review of Assessing and Managing Risks (E-MRP, E-IPS)

The key management practices for assessing and evaluating the system of internal controls in an enterprise are given as follows:

Ensure that assurance providers are independent and qualified: Ensure that the entities performing assurance are independent from the function, groups or organizations in scope.

The entities performing assurance should demonstrate

an appropriate attitude and appearance,
competence in the skills and knowledge necessary to perform assurance, and
adherence to codes of ethics and professional standards.

Monitor Internal Controls: Continuously monitor, benchmark and improve the IT control environment and control framework to meet organizational objectives.

Review Business Process Controls Effectiveness: Review the operation of controls, including a review of monitoring and test evidence to ensure that controls within business processes operate effectively.

It also includes activities to maintain evidence of the effective operation of controls through mechanisms such as
periodic testing of controls,
continuous controls monitoring,
independent assessments,
command and control centers, and
network operations centers.

Perform Control Self-assessments: Encourage management and process owners to take positive ownership of control improvement through a continuing program of self- assessment to evaluate the completeness and effectiveness of management's control over processes, policies and contracts.

Execute assurance initiatives: Execute the planned assurance initiative.

Report on identified findings.

Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control system residual risks.

Identify and Report Control Deficiencies: Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.

Plan Assurance Initiatives: Plan assurance initiatives based on

Enterprise, assurance and conformance objectives,
strategic priorities,
inherent risk resource constraints, and
sufficient knowledge of the enterprise.

Scope assurance initiatives: Define and agree with management on the scope of the assurance initiative, based on the assurance objectives.