CHAPTER 1

CONCEPT OF GOVERNANCE AND MANAGEMENT OF INFORMATION SYSTEM

1. KEY CONCEPT OF GOVERNANCE:

In this changing environment, enterprises have to adapt itself. Senior management is responsible for ensuring that right structure of decision making accountabilities are shared among people in the enterprise and where accountability is shared, governance comes into force.

Now let us move towards various aspects used in this concept:

A. GOVERNANCE:

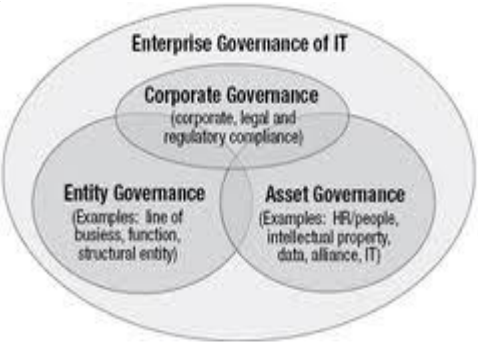
-- Derived from Greek word meaning "To steer".

-- Governance: All means and mechanism that will enable stakeholder to have an organised mechanism for evaluation, monitoring compliances and performance.

B. ENTERPRISE GOVERNANCE:

-- Defined as: Set of responsibilities & practices exercised by the board and executive management to ensure proper monitoring, objectives are achieved, risks are managed properly.

-- It is framework into which many tools, techniques and codes of best practices can fit.


Enterprise Governance of IT
Corporate Governance
(corporate, legal and regulatory compliance)
Entity Governance
(Examples: line of busiess, function, structural entity)
Asset Governance
(Examples: HR/people, intellectual property, data, alliance, IT)

C. CORPORATE GOVERNANCE:

-- Defined as: System by which a company or enterprise is directed & controlled to achieve the objectives of increasing shareholder value by enhancing the economic performance.

-- Refers to: Structure and processes for direction and control of companies.

Corporate governance is all about ensuring that companies act in the best interests of their owners -- the shareholders -- who have invested their savings, their children's college funds or their retirement funds in the company. Corporate governance is also about considering the interests of other entities impacted by the company -- employees, the environment and even communities.

Toyota is a global leader in automotive sales, technology and production while also retaining one of the world's most recognizable and highly valued brands. At the heart of their success is the innovative and ground breaking production methods made possible by the company's recognition of the value of employee empowerment. At Toyota, the company has employed these proven techniques of co-determination to encourage employee and supplier involvement in their decision making process, since these practices "help improve both the ability and attitude" of stakeholders

CA AKHIL MITTAL

2. CORPORATE GOVERNANCE AND IT GOVERNANCE:

Management is of the view that IT is an important part to achieve the organisational objectives. IT provides critical inputs to meet the information need of stakeholders. Hence corporate governance drives and sets IT governance.

"IT GOVERNENCE": System by which IT activities are directed and controlled to achieve business objectives. Hence it can be said that there is an inseparable relationship between corporate governance and IT governance or **IT Governance** is a sub-set of Corporate/enterprise governance.

BENEFITS OF GOVERNANCE:

1. Achieving enterprises objectives by combining all aspects of the business and ensures transparent decision rights and accountability framework.
2. Implementing & integrating business processes into enterprises.
3. Enabling effective & strategically aligned decision making (defining IT role, architecture, service portfolio etc.)
4. Improving customer, business relationship and reducing internal strife (angry or bitter disagreement over fundamental issues) by integrating customer, business and external IT providers.

GOVERNANCE DIMENSION:

Enterprise governance constitutes entire framework of organisation. Governance has 2 dimensions:

1. **CONFORMANCE/CORPORATE GOVERNANCE:**
   --This focus on regulatory requirements.
   --This covers issues like role of chairman, CFO, board of directors composition, control assurance, risk management for compliance.
   --These are established oversight mechanism to ensure that good corporate governance processes are effective.
   --The conformance dimension is monitored by the audit committee.
   --Example: **Sarbanes Oxley Act of US, Clause 49 of listing agreement.**

2. **PERFORMANCE OR BUSINESS GOVERNANCE:**
   --This focus on strategy and value creation with the objectives of helping the board to make the strategic decisions,
   --This approach or dimension doesn't restrict itself to the standards, it rather advisable to develop appropriate practices, tools and techniques.
   --The performance dimension is whole-sole responsibility of the board.

CA AKHIL MITTAL

3. IT GOVERNANCE AND GEIT:

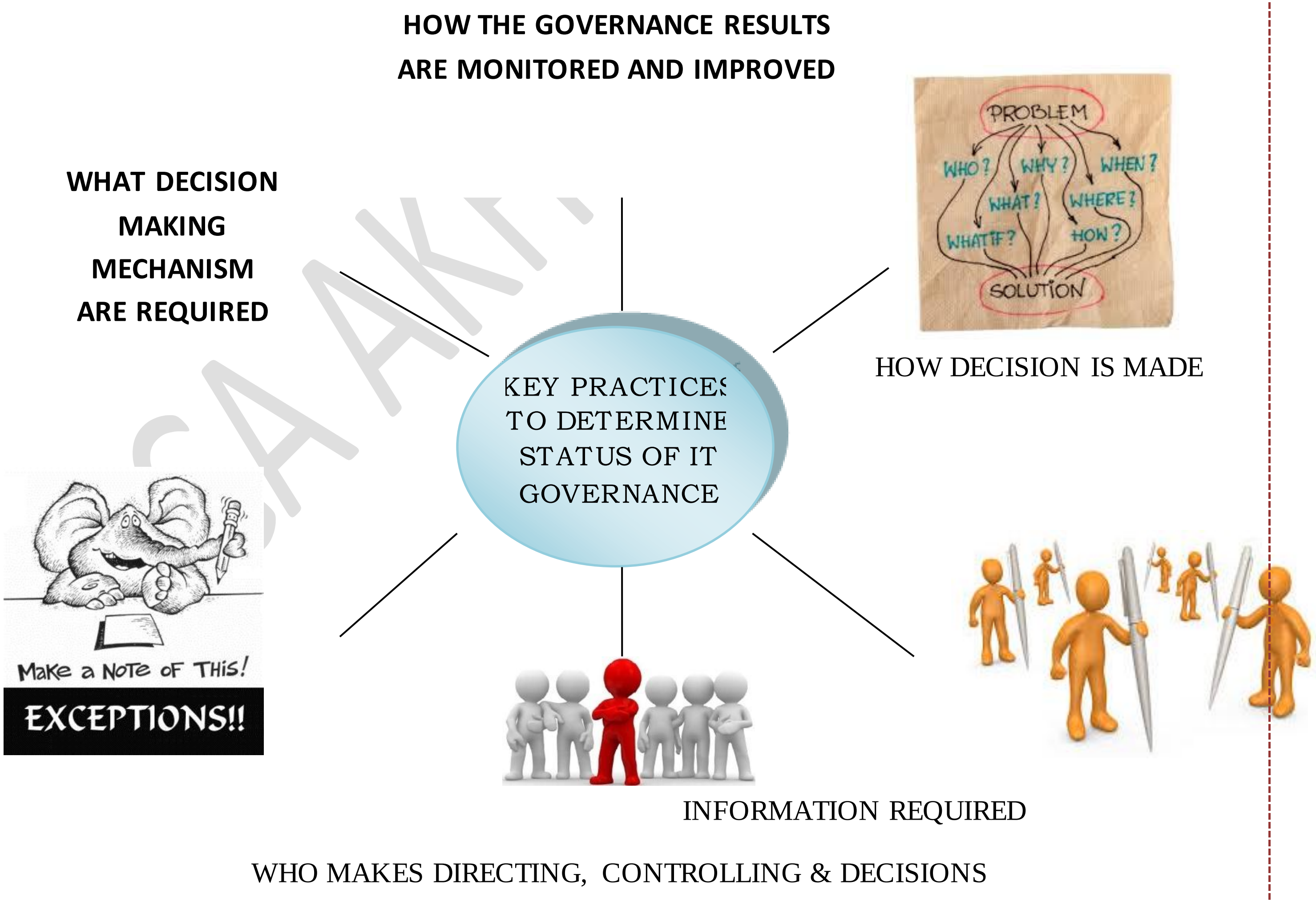
First of all, everyone will be wondering what is GEIT!!!..... So here's the definition:
"GEIT" : **GOVERNANCE OF ENTERPRISE IT.**
However, IT governance and GEIT are used interchangeably, but GEIT is macro in term and a broader concept.

IT GOVERNANCE:

OBJECTIVE:
The objective is to determine and cause the desired behaviour and results to achieve the strategic impact of IT.

DEFINITION:
System by which IT activities are directed and controlled to achieve business objective. Hence it can be said that there is an inseparable relationship between corporate governance and IT governance or **IT Governance** is a sub-set of Corporate/enterprise governance.

KEY PRACTICES TO DETERMINE STATUS OF IT GOVERNANCE:


HOW THE GOVERNANCE RESULTS ARE MONITORED AND IMPROVED
WHAT DECISION MAKING MECHANISM ARE REQUIRED
PROBLEM
WHO?
WHY?
WHEN?
WHAT?
WHERE?
WHAT IF?
HOW?
SOLUTION
HOW DECISION IS MADE
KEY PRACTICES TO DETERMINE STATUS OF IT GOVERNANCE
Make a Note of This!
EXCEPTIONS!!
INFORMATION REQUIRED
WHO MAKES DIRECTING, CONTROLLING & DECISIONS

BENEFITS OF GOVERNANCE:

1. Increased value delivered through enterprise IT.
2. Increased user satisfaction with IT services.
3. Better cost performance of IT.
4. Improved transparency and understanding of IT.
5. Improved compliance with law.

GEIT GOVERNANCE: (यहाँ पर corporate governance और IT साथ में काम करते है

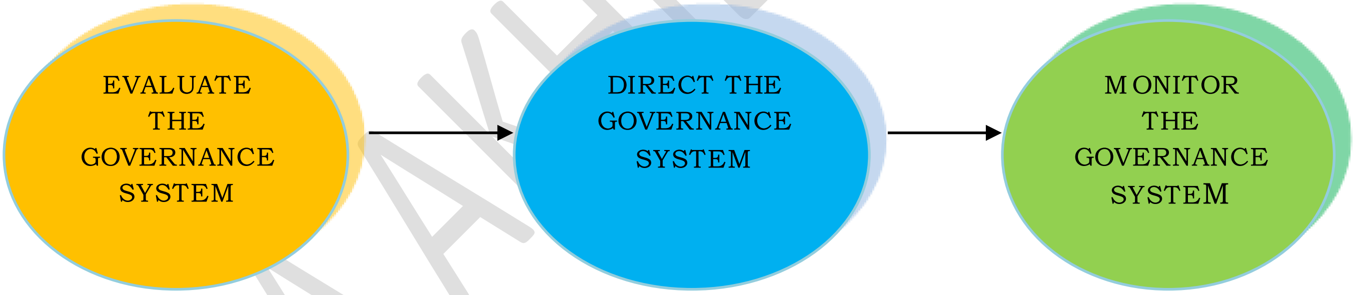
Governance of enterprise IT (GEIT) is a sub set of corporate governance & facilitates implementation of IS control framework.

Its objective is to analyze and articulate (Expressing oneself easily in clear and effective language) the requirement for governance of enterprise IT.

BENEFITS OF GEIT: (CODE TO REMEMBER : M.A.R.E.)

1. **M**onitoring: The IT related processes are seen effectively and transparently.
2. **A**pproach: Ensures consistency in approach and in alignment with enterprises strategy.
3. **R**equirements are met: Ensures governance requirement of board are met.
4. **E**nsures that IT related decisions are taken in tune with enterprise strategy.

KEY GOVERNANCE PRACTICES OF GEIT:



EVALUATE THE GOVERNANCE SYSTEM → DIRECT THE GOVERNANCE SYSTEM → MONITOR THE GOVERNANCE SYSTEM

System का मूल्यांकन करें

system को build up करो

system प्को मॉनीटर करो

A. **Evaluate the governance system**:

-- Have communication with stakeholders, document the requirements,
-- Make judgement on the current and future design of the governance of enterprise IT.

B. **Direct the governance system:**

--Inform leader and obtain their support.
--Guide the structures, processes and practices in line with agreed governance principle, decision making principles.

CA AKHIL MITTAL

C. Monitor the governance system:

-- Monitor the effectiveness and performance of the enterprises governance of IT.
-- To ascertain whether the mechanism is working efficiently or not.

4. CORPORATE GOVERNANCE, ERM AND INTERNAL CONTROLS:

CORPORATE GOVERNANCE is defined as a system by which a company or enterprise is directed & controlled to achieve the objectives of increasing shareholder value by enhancing the economic performance.

There is an urge of mandating the implementation of corporate governance integrated with the ERM and internal controls. The corporate governance specifies the **DISTRIBUTION OF RIGHTS** and responsibilities of different participants such as **BOARD, MANAGER, and SHAREHOLDER ETC.**

Some of the best practices of corporate governance:

A. Assignment of responsibilities (काम का वितरण):

-- Clear assignment of responsibilities and decision making authorities.
-- Incorporating hierarchy of required approvals.

B. Cooperation between participants (कंपनी के अधिकारियों के बीच सहयोग):

-- Establishing mechanism for interaction and cooperation,
-- Among board of director, senior management and others.

MONITORING THING (चेक या नजर रखने के लिए):

C. Implementing strong internal control system, including external/internal audit functions.
D. Special monitoring of risk exposure.

OTHER POINTS:

E. Financial incentive to senior management, business line management and employees.
F. Appropriate information flows internally and to public.

ENTERPRISE RISK MANAGEMENT (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress.

It is process affected by entity's board of directors, personnel and management.

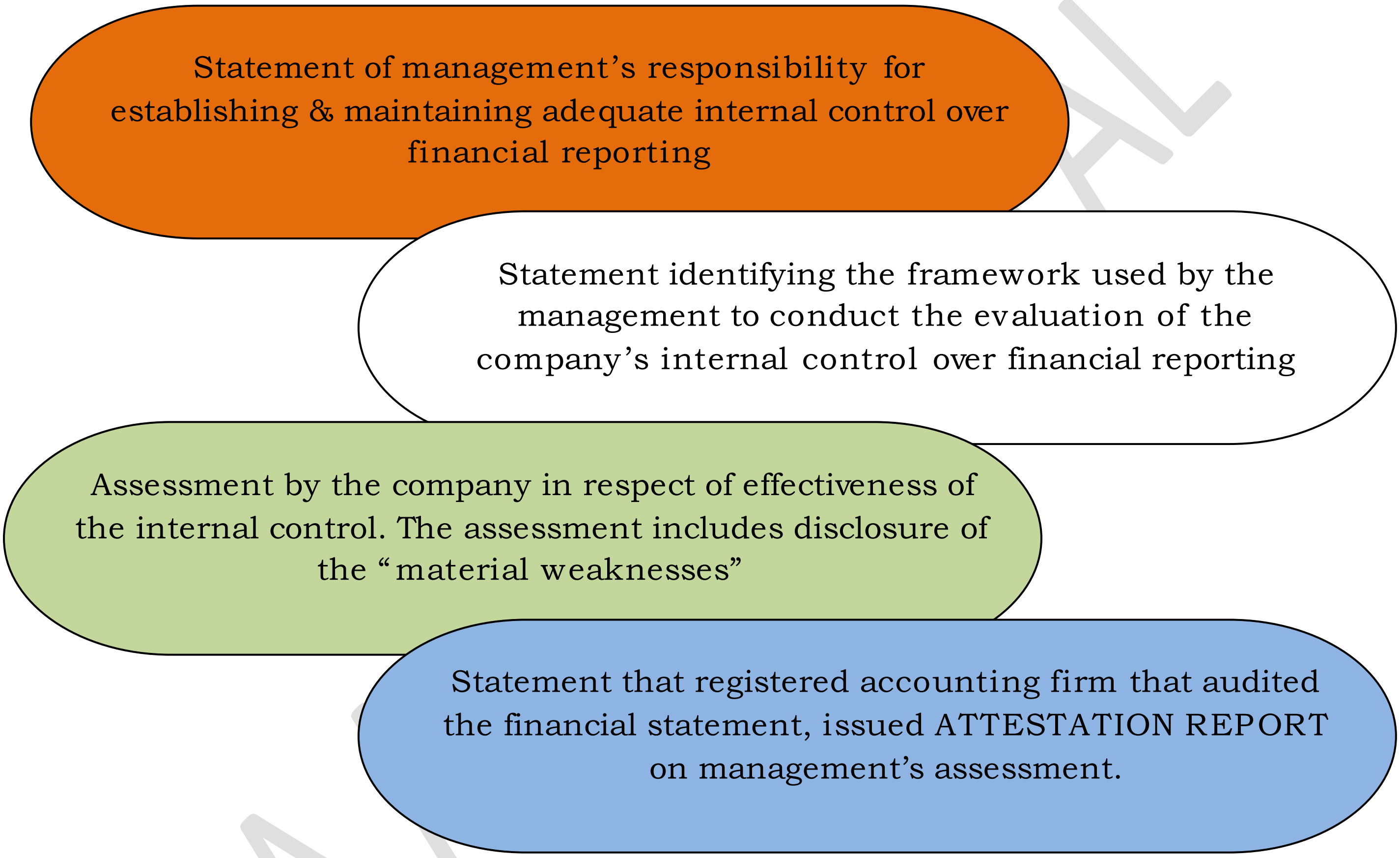
INTERNAL CONTROLS Securities and Exchange Commission defines **"INTERNAL CONTROLS OVER FINANCIAL REPORTING" as** a process designed under the company's principal executive and finance officer.

CA AKHIL MITTAL

Company management must provide reasonable assurance regarding the reliability of the financial statement & reporting for external purposes as per general accepted accounting principles and policies & procedures:

-- For maintenance of records with reasonable details and accuracy.
-- Provide reasonable assurance that transactions are recorded to permit preparation of the financial statement with generally accepted accounting principles.

Under final rules, a company audit report must contain report on internal control of management containing:



Statement of management's responsibility for establishing & maintaining adequate internal control over financial reporting

Statement identifying the framework used by the management to conduct the evaluation of the company's internal control over financial reporting

Assessment by the company in respect of effectiveness of the internal control. The assessment includes disclosure of the " material weaknesses"

Statement that registered accounting firm that audited the financial statement, issued ATTESTATION REPORT on management's assessment.

A. Responsibility for implementing Internal Control:

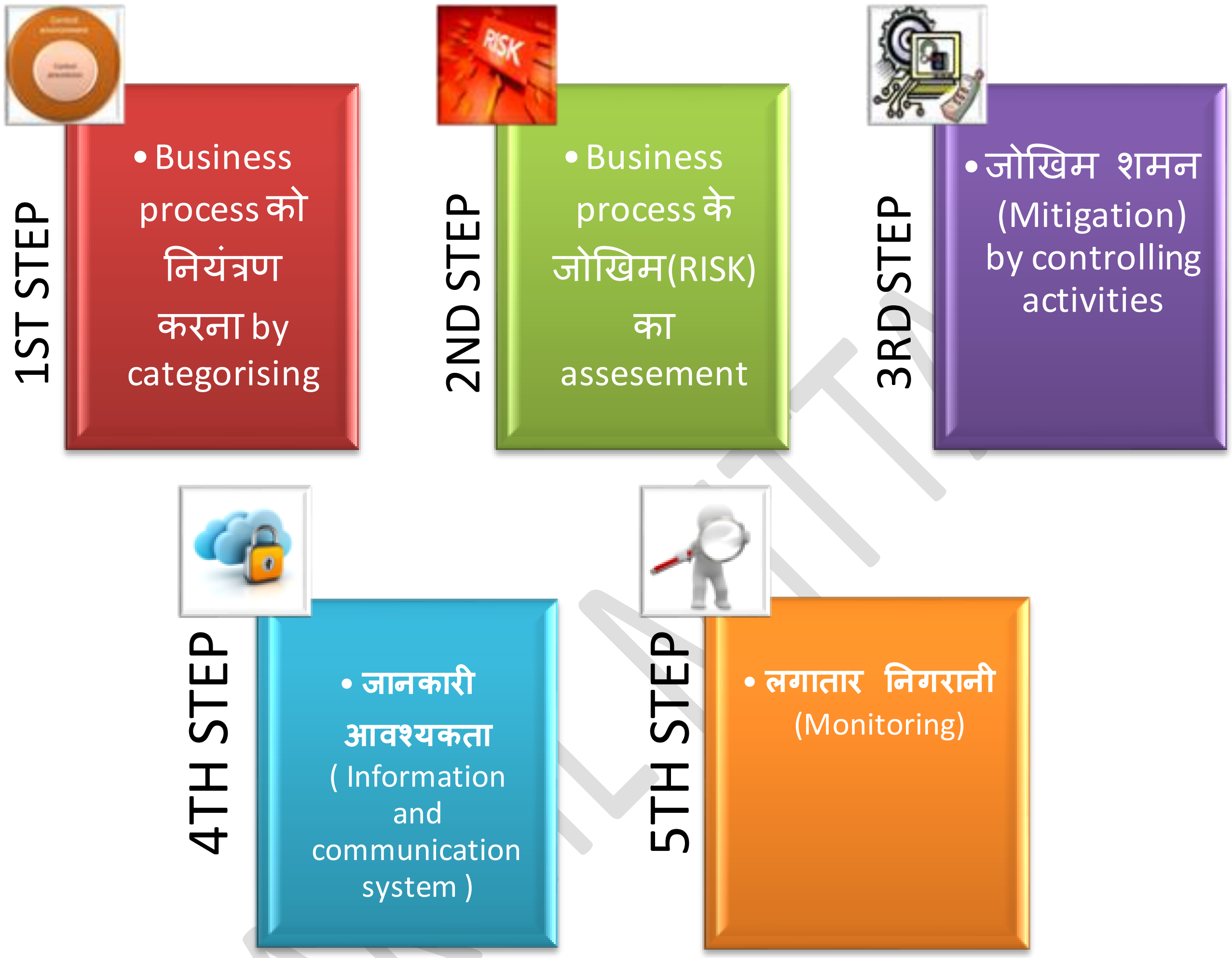
-- SOX make major changes by holding CFO's and CEO's,
-- Towards quality & effectiveness of their organisation's internal controls.

-- Internal controls are expected to provide reasonable assurance to the entity.

-- An organisation ensures that financial statements comply with **financial accounting standards & International accounting standards.**

B. Internal Control as per COSO:

In an computerised environment, organisation can achieve data integrity, system efficiency only organisation sets up a system of internal controls. Internal controls comprises of 5 inter-related components:



1ST STEP

- Business process को नियंत्रण करना by categorising

2ND STEP

- Business process के जोखिम(RISK) का assesement

3RD STEP

- जोखिम शमन (Mitigation) by controlling activities

4TH STEP

- जानकारी आवश्यकता (Information and communication system)

5TH STEP

- लगातार निगरानी (Monitoring)

CA ANKITA

1. **Control Environment:**
   -- Entity need to develop and maintain controlled environment,
   -- Including categorising the business process on materiality/criticality basis.

2. **Risk assessment:**
   -- Each business process is associated with some risk.
   -- As such there is necessity of regular assessment of the risks.

3. **Control activities:**
   -- Control activities must be developed to **manage, mitigate and reduce**
   -- Risk associated with business processes.

4. **Information and communication:**
   -- Information and communication system is needed to capture & exchange,
   -- Information needed to conduct, manage and control business processes.

5. **Monitoring:**
   -- Internal control processes must be continuously monitored;
   -- And adaptable to changing conditions

C. Clause 49:

- Clause 49 of SEBI also mandates the implementation of ERM and internal controls.
- Holds senior management responsible legally for the implementation.

5. ROLE OF IT in ENTERPRISES:

In today corporate scenario, IT is not confined for the data processing but also it has some competitive advantages too.

Online transactions, MIS, decision support system are the extended uses of IT technology. Now-a-days, IT is used to perform business processes, activities and tasks.

A. Business and IT strategy:

--Management strategy determines at macro level,
--The path and methodology of rendering services at macro level.
--**Strategy** is formulated by senior management.
--Policies and procedures are formulated on strategy,
--Both business and IT strategy complement each other.

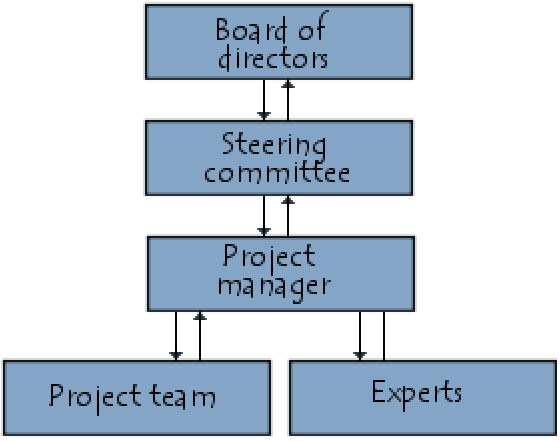
Every enterprise irrespective of the size needs an effective internal control system. Controls **are the policies and procedures that assure business objectives will be achieved and undesirable events will be being prevented, corrected.**

Role of the auditor is to ensure that internal controls implemented are working as desired. However, auditor role is of immense important at the time of implementing these controls. This requires that auditor must have good understanding of the concept of enterprise strategy.

B. IT steering Committee:

Planning is needed for determining and monitoring the achievement of the enterprise goals. Management needs information for crucial decisions, so the element of planning is an essential part of developing effective information system.

As such there is equal involvement of senior management and IT persons.



"IT STEERING COMMITTEE": **Led by the board of director and comprises of functional head from all the departments.**

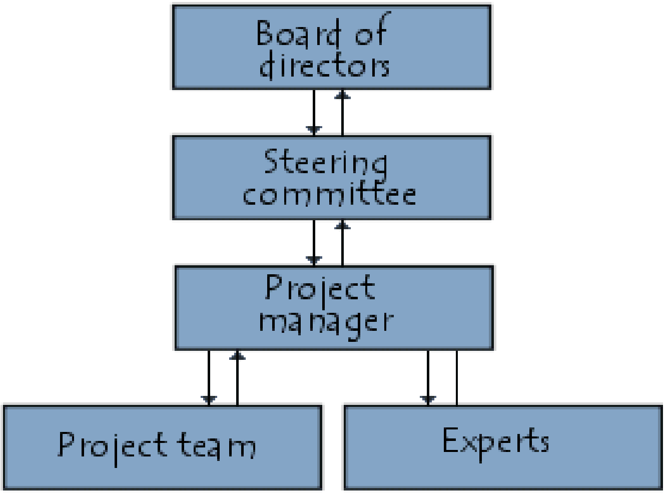
CA AKHIL MITTAL

As it is shown in the above diagram that board of directors are on the driving wheel, so we can evaluate the working and accountability flow:

1. **Roles & responsibilities of steering committee must be documented and approved by the senior management.**

2. **All the department heads will be responsible for the decision taken for their respective departments.**

3. **IT steering committee provides direction to deploy IT and information system in the enterprises.**



Following are the key functions of IT steering committee:

-- To ensure long & short term plans of IT department are in tune with the organisation objectives and goals.

-- To review and approve standards, policies & procedures.

-- To establish size and scope of IT functions & set priorities.

-- To review & approve IT deployment projects in all stages.
-- To make decision on IT deployment & implementation.
-- To facilitate implementation of IT security within enterprise

CA AKHIL MITTAL

6. IT STRATEGY PLANNING:

Why we plan: **Planning** is the process of thinking about and organizing the activities required to achieve a desired goal.

1. Management must ensure that IT long and short term plans are communicated to business process owners.
2. Management should establish processes to capture & report feedback from business owners.

IT STRATEGY PLANNING PROCESS

IT STRATEGY PLANNING

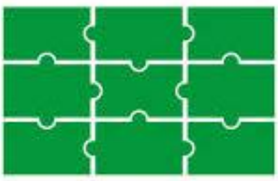
--Planning process must be dynamic in nature.
--Process owner must ensure that process must be in place to ensure modification in IT plans as per change in IT conditions.
--It must be ensured that IT function resources are allocated on basis consistent with the long term plan.

STRATEGIC PLANNING

-- Refers to planning undertaken by the top management,
-- Towards meeting long term objectives of the enterprises.

There are **3 levels of managerial activity** in an enterprise:

STRATEGIC PLANNING CYCLE



Management Control Framework

Operations
Fault Analysis
Monitor
Control
Load Control
Reporting & Statistics
Analysis
Network Operations
Maintenance & Construction
Financial
Supply Chain / Logistics
Extension Planning
Ops Planning
Records & Assets
Meter Reading & Control
Communications Network
Security Management
Markets
Service Provider
Customer
Transmission
Distribution
External Communication Interface
Internal Communication Interface
Electrical Interface
Domain

CA AKHIL MITTAL

Now explaining each of the aforesaid levels:

STRATEGIC PLANNING

STRATEGIC PLANNING

Strategic planning refers to:

-- Process by which top management determines overall,

-- Organisational objectives and purposes,

-- & how they are to be achieved.

Corporate Strategic planning refers to:

-- Determining the overall character & purpose of organisation.

-- Business it will enter, allocation of the resources.

IT Strategic planning in enterprises can be classified into 4 categories:

1. **ENTERPRISE STRATEGIC PLAN:**

-- This plan encompasses the overall charter of the enterprises under which all units, including information systems must operate.

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

-- Following procedure is followed:

1. Statement of mission.
2. Specification of strategic objectives.
3. Assessment of environmental & organisational factors.
4. Statement to achieve organisational objectives.
5. Listing of the priorities.

2. **INFORMATION SYSTEMS STRATEGIC PLAN:**

-- IS strategy focus on striking balance between IT opportunities & business requirement.

-- It requires strategic planning process to be undertaken at regular interval for long term planning. And this plans to be translated into operational plans.

-- Enablers of IS strategic plan are:

रणनीति बनाने → IT infrastructure एंड technology बनाना → feasibility check → Mgmt. support

1. Enterprise business strategy. -- **रणनीति बनाने**

2. How IT supports business objectives.
3. Inventory of technical solution & infrastructure.
4. Monitoring of technology markets.

} -- **IT infrastructure एंड technology बनाना**

5. Feasibilities checking.

6. Need for senior management buy-in, support and critical review.

3. **INFORMATION SYSTEMS REQUIREMENT PLAN:**

Enterprise needs to have defined information structure so as to optimise the requirement from the information system. So, business has to ensure that business information model
Have to be reviewed periodically to optimise the use of the information.

We will study that a system has to be build up on the requirement of the users. Similarly, IS requirement plan has to be drawn on the basis of information architecture requirements.
Following are the enablers of information architecture:

CA AKHIL MITTAL

INFORMATION SYSTEM OF THE ORGANISATION

It contains:

1. Information model representing the business.
2. Enterprise का information architectural standards.
3. Data repository and dictionary.
4. Data syntax rules.
5. Data ownership & security classifications.

How to remember the above points:

1. Information model business में मौजूद है! 2. Information system का standard is there.

3. Information system में DATA है so repository and depository and syntax rule too.

4. यह DATA protect करना है !

AKHIL MITT

4. INFORMATION SYSTEMS APPLICATIONS AND FACILITIES PLAN:

On the basis of information systems architecture, management can develop an information systems applications and facilities. The plan includes:

A. Application system to be developed & preparation of time schedule.
B. Hardware & software acquisition & development.
C. Facilities required.
D. Organisation changes required.

Now in this case some questions arise….!!!

WHO IS RESPONSIBLE FOR THE PLANS

The senior management is responsible for developing and implementing the long & short term missions and goals. Also management must ensure that IT issues are considered while making plans.

PERIOD OF THE PLANS

The strategic plan period vary from 1-3 years.

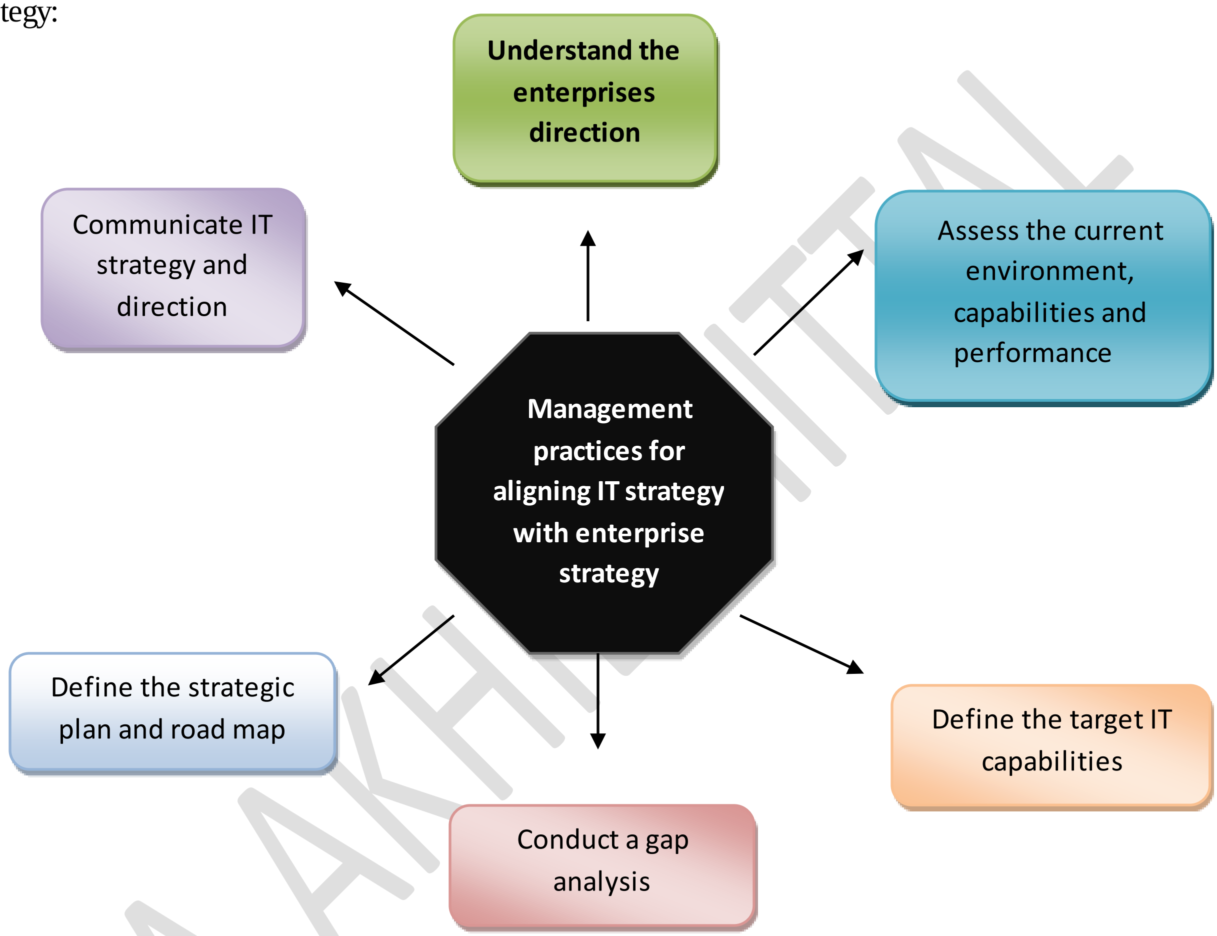
Strategic planning facilities in putting organisational objectives into time bound plans and action. Comprehensive planning helps to ensure an effective and efficient enterprise.

OBJECTIVE OF IT STRATEGY:

-- Primary objective is to **provide holistic view of IT environment.**
-- Alignment of strategic IT plans with business objectives is done by clearly communicating the objectives and associated accountabilities, so all understand their responsibilities.

But how to align the IT strategy and business objectives:

There are few key management practices, which are required for aligning IT strategy with the enterprise strategy:


Management practices for aligning IT strategy with enterprise strategy
Understand the enterprises direction
Assess the current environment, capabilities and performance
Define the target IT capabilities
Conduct a gap analysis
Define the strategic plan and road map
Communicate IT strategy and direction

CA AKHIL MITTAL

1. **Understand enterprise direction:**
   -- Consider current environment as well as enterprises future strategy & objectives.
   -- It also includes considering the external environment like regulations, industry drivers etc.

2. **Assess the current environment, capabilities and performance:**
   -- Consider current internal business & IT capabilities and external IT services.
   -- Develop the understanding of the enterprise architecture in relation to IT.
   -- Identify the issues currently dealt with and the ways of improvements.

3. **Define the target IT capabilities:**
   --Define the target business and corresponding IT capabilities & IT services.
   --It involves complete understanding of the enterprises and its both internal and external environment. It also involves consideration of standards, best practices etc.

4. Conduct a gap analysis:

-- Identify the gap between the target and current environments and consider the alignment of assets with business outcomes,

-- To optimise the investment and utilisation of internal & external asset base.

5. Define the strategic plan and road map:

-- Entrepreneur has to prove the nexus between the IT capabilities will contribute to the organisational goals.

-- Explain as to how IT will support IT enabled investments, processes, assets etc.

-- Now important thing that how IT will initiate the actions to close up the gaps is an important consideration.

6. Communicate IT strategy and direction:

-- In earlier phases, it has been decided what to do and what is needed to achieve the objectives.

-- Now for effective implementation of the strategies it is important to communicate the same to the appropriate stakeholders and users throughout the enterprise

BUSINESS VALUE FROM USE OF IT (INFO. TECHNOLOGY):

Business value is achieved from the use of IT by ensuring the optimisation of value contribution to business from business processes, IT services and IT assets resulting from IT enabled investments at an acceptable cost. Following are the key management practices needed to be followed for the evaluation "whether business value is derived from IT":

Alignment of IT services and business objectives: (IT का कारोबार उद्देश्यों के साथ गठबंधन)

1. Evaluate the value optimisation: (Whether goals are achievable with IT assets)

-- Evaluate the portfolio of IT enabled investments, services and assets to determine the likelihood of achieving organisational objectives.

-- The objectives and delivering the values at reasonable cost is the main point of value optimisation.

2. Direct value optimisation: (Extract the maximum from IT assets)

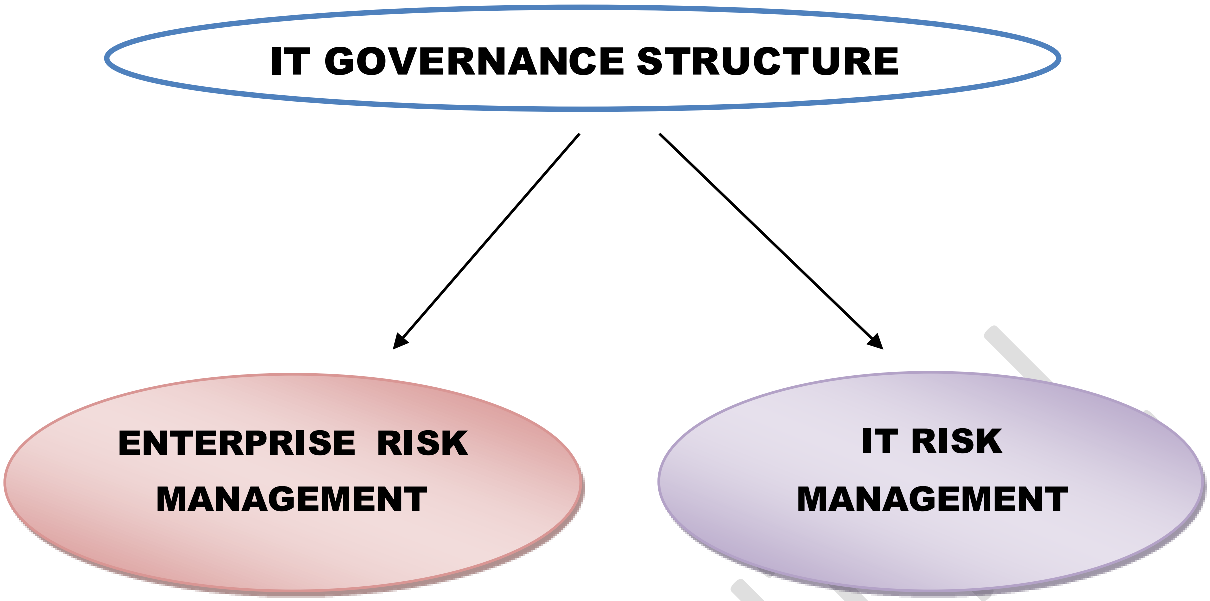
- Direct value management principles aimed at optimal value optimisation from the IT enabled investments throughout their economic life.

3. Monitor value optimisation: (Monitoring the benefits from IT services)

-- Monitor the key goals to determine the extent to which business is generating the expected value from IT enabled investments and services.

CA AKHIL MITTAL

7. RISK MANAGEMENT:



CA AKHIL MI

Effective IT governance helps to ensure close linkage to the enterprises and IT risk management. IT governance is an integral part of corporate risk management. There must be a procedure to communicate the status of risks involved to key stakeholders so as to ensure that proper steps can be taken up.

INFORMATION TECHNOLOGY RISK AND RISK MANAGEMENT:

IT environment is changing day by day and it is essential for the enterprise to better manage IT related risks. Business processes are indeed based upon electronic information and IT system is essential to support critical business processes.

RISK: It is possibility of something adverse happening, resulting in loss or exposure.

RISK MANAGEMENT: Process of assessing risk and taking steps to reduce it to acceptable level.

Now we are talking about the risk but what are the sources of risk?? **(जोखिम के स्रोत)**

The most important step in risk management is to identify the **SOURCES OF THE RISK**, the areas from which they occur. Some of the common sources of risks are:

BUSINESS RELATED	**OTHER FACTORS**
-- Commercial and legal relationship	-- Human Behaviour
-- Technology and technical Issues	-- Natural Events
-- Management Activities and Controls	-- Individual Activities

RELATED TERMS TO RISK MANAGEMENT:

ASSETS:

Asset can be defined as something of value to the organisation. Example information in e-form, software system, employees...Following are the characteristics of the assets:

1. Recognised to be value to the organisation.
2. Assets can't be replaced without cost, skills and time.
3. They form the part of organisation's corporate identity.
4. They are capable of distinguishing the information level i.e. confidential, proprietary etc.

VULNERABILITY:

-- It is the weakness in the system safeguard that exposes system to THREATS.

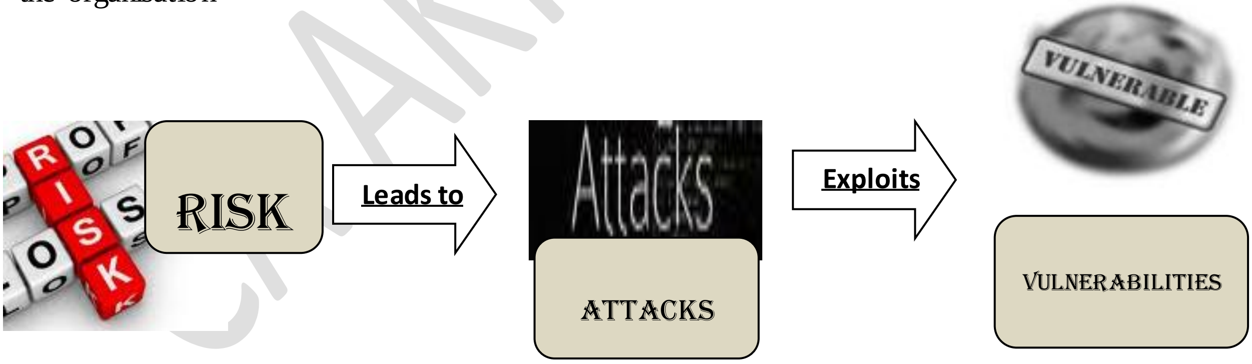
-- Examples on vulnerability:
-- Leaving door unlocked makes the house vulnerable to theft.
-- Use of short passwords which are prone to cracking or hacking

-- We have studied about the vulnerability and examples. But why vulnerabilities arise..!!!

THREATS:

-- Any entity, circumstances with the potential to harm the software system or component through unauthorised access, destructions or modifications

-- It is an action, event or condition **where there is compromise** in the **quality and ability** to harm the organisation



-- Threats exists where there is asset. Asset is nothing but the data contained in information system.

I am hereby enumerating the characteristics of the threat:

❖ It is action/event/condition where there is a compromise in the system

❖ Negative impact on the quality of the system.

❖ Threat has the capability to attack on the system with the intent to harm it.

CA AKHIL MITTAL

EXPOSURE:

-- It is the extent of the loss to the organisation when a risk materialised (occurs).

-- For instance, loss of business, loss of reputation, violation of the privacy etc.

LIKELIHOOD: (संभावना)

-- It is the estimation of probability that threat will succeed in achieving undesirable threat.

ATTACK:

-- It is the set of action designed to compromise confidentiality, integrity & availability of an information system.

-- It is an attempt to gain unauthorised access to the system services. In software terms, an attack is a malicious intentional fault that has intent of exploiting vulnerabilities.

RISK:

-- It is likelihood that an organisation would face vulnerability becoming harmful.
-- Risk analysis is a process of identifying the magnitude of the risk and their impact on entity.
-- Risk assessment includes the following:

-- Identifying the threats and vulnerabilities in the system. (संभावित खतरों की पहचान करना.)

-- Impact of threats on the CIA (confidentiality, integrity & availability) **of information system.**

-- Identification & analysis of security controls for information system.

-- Information system can generate many direct and indirect risks. These risks creates gap between **need to protect system & degree of protection** applied.

- The gap is caused by:
  - **Devolution of management & control**
  - **Interconnectivity of systems**
  - **Elimination of distance, time and space as constraints**
  - **Technology usage is more**

CODE TO REMEMBER: **D.I.E.T.**

COUNTER MEASURE:

An action, device, procedure, technique that reduces the vulnerability of a system or Component is referred as counter measure.

OWNER:

1. Wish to minimise the risk by applying countermeasure.
2. Owner must value the assets he posses.
3. Owner must impose counter measure to reduce risk.

CA AKHIL MITTAL

THREAT AGENT:

1. Threat agents give rise to threats,
2. That increases the risk IRO assets that may damage the system.

-- RESIDUAL RISK: Any risk remaining after the counter measures are analysed & implemented.

RISK MANAGEMENT STRATEGIES:

When risks are identified and analysed, it is important to know how to deal with them. It means if threat is minor then it will be useless to implement expensive control processes against them. Risk management strategy is explained as below:

Now I am explaining the same in HINDI, the ways to manage the risk:

1. जोखिम पर ध्यान न दें
2. जोखिम शेयर करना
3. जोखिम को स्वीकार करना
4. जोखिम को कम करना
5. जोखिम को समाप्त करना

CODE TO REMEMBER

T-S.A.M.E

Now same in Detail: (please relate the above points with the given below points)

1. **Turn Back:** (जोखिम पर ध्यान न दें)

-- Where the probability and impact of risk is low, then management may ignore such risks.

1. **Share the risk:** (जोखिम शेयर करना)

-- One way to manage the risk is to share the risk with the trading partner or the suppliers.

-- Example: Supplier mitigates the risks associated with IT infrastructure management by outsourcing it to company having expertise in the IT infrastructure management.

2. **Accept the Risk:** (जोखिम को स्वीकार करना)

-- Some of the risks are so minor that their impact & probability of occurrence is low.

-- In this case it is desirable to run the business instead of establishing costly procedure to mitigate the risk (minor).

3. **Mitigate the Risk:** (जोखिम को कम करना)

-- Where other options are not available it is advisable to devise suitable controls.

-- To prevent the risk from manifesting (reveal) itself and to minimise the impact.

4. **Eliminate the Risk:** (जोखिम को समाप्त करना)

-- It is possible to associate risk with particular technology or vendor.

-- SO it will be advisable to replace the technology and to seek more capable suppliers.

CA AKHIL MITTAL

RISK MANAGEMENT IN COBIT 5:

COBIT framework provides excellent management strategy and practices from governance and management practices.

The governance domain contains 5 governance processes, one of which focuses on the stakeholders risk related objectives.

EDM03: Ensure Risk Optimization

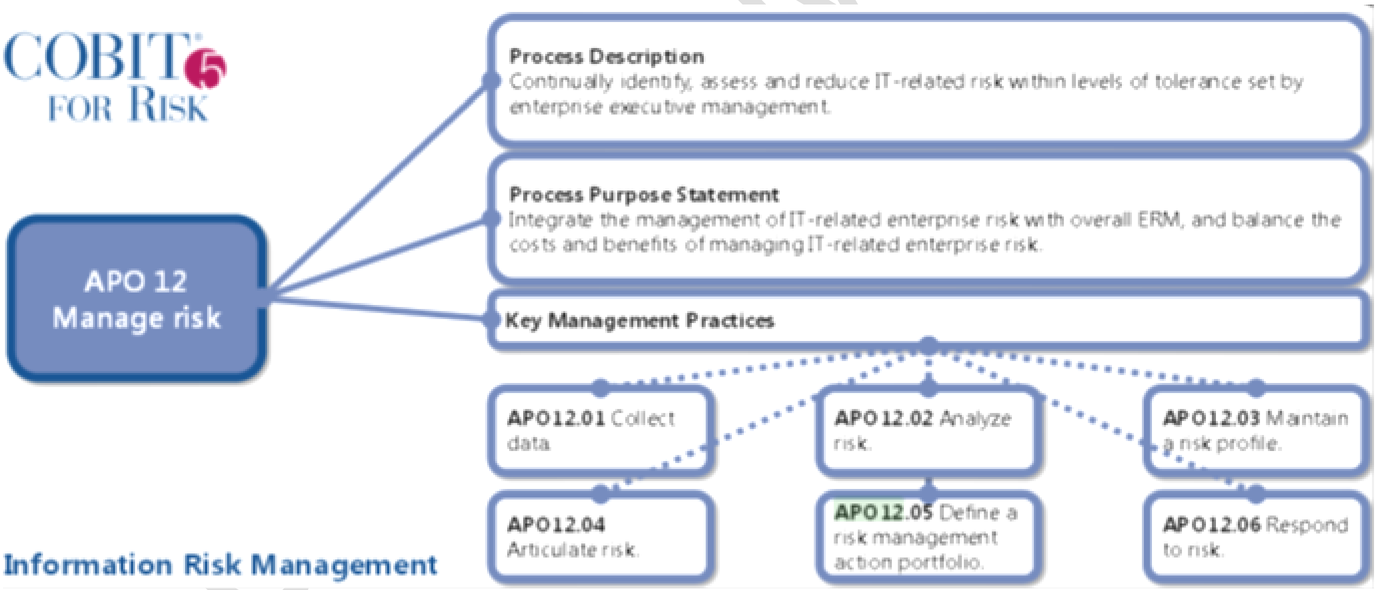
Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage, monitor and communicate IT-related business risk, and that the framework for IT risk management is in alignment with the enterprise risk management (ERM) framework.

-- Ensures that enterprise risk appetite and tolerance are understood, communicated.
-- Provide guidance on how to ensure IT related risks doesn't exceed risk appetite & tolerance.
-- Impact of IT risk to enterprise is identified and managed.

MITTAL

AP012: Align, Plan and Organize

Ensure that an IT risk management framework exists to identify, analyze, mitigate, manage,



Process Description
Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Process Purpose Statement
Integrate the management of IT-related enterprise risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.

Key Management Practices

- **APO12.01** Collect data.
- **APO12.02** Analyze risk.
- **APO12.03** Maintain a risk profile.
- **APO12.04** Articulate risk.
- **APO12.05** Define a risk management action portfolio.
- **APO12.06** Respond to risk.

--This process requires continually identifying, assessing and reducing IT related risk within tolerance levels set up by the enterprise executive management.

--This process aims to integrate management of IT related enterprise risks with ERM (enterprise risk management) and balance the benefit and cost of managing IT related risks.

Now for the effective risk management it is imperative to combine the

EDM03: Ensure Risk Optimization
&
AP012: Align, Plan and Organize

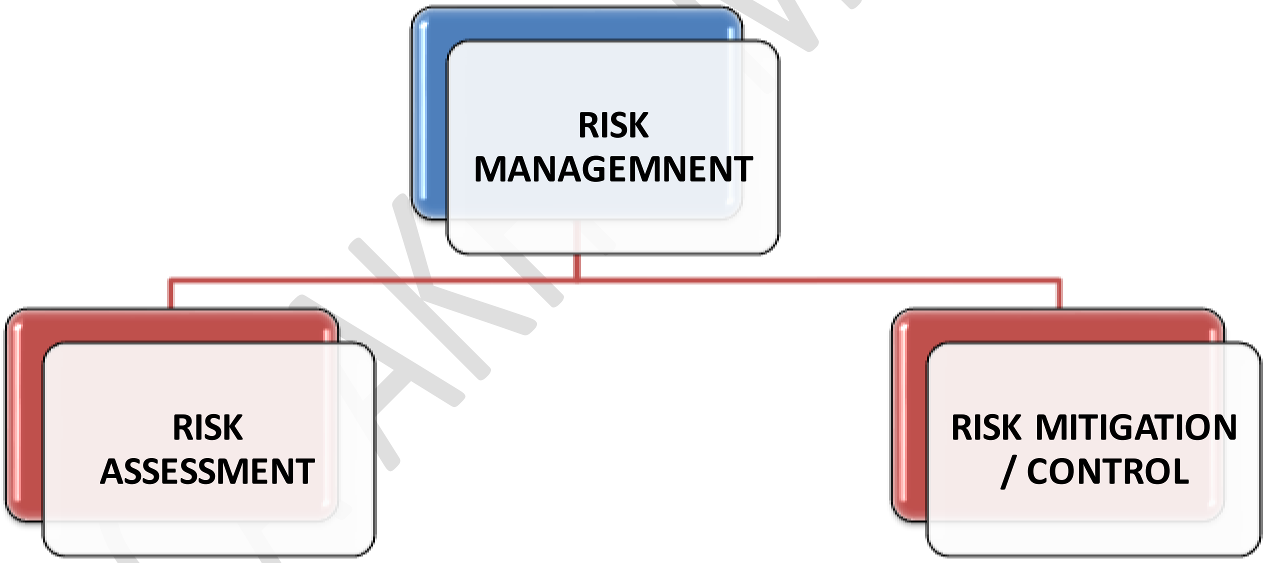
EDM 03 & APO12

Must ensure that risk management covers the life cycle and covers both governance and management perspective.

EDM03: Stakeholder approach to risk and to direct how risks facing the enterprise will be treated.

APO12: Stakeholder direction is being followed by the enterprise in ERM arrangements.

Following is the diagrammatic representation of the scope of risk management concept:



RISK MANAGEMNENT

RISK ASSESSMENT

RISK MITIGATION / CONTROL

-- RISK IDENTIFICATION

-- RISK ANALYSIS

-- RISK PRIORITIZATION

-- RISK REDUCTION

-- RISK PLANNING

-- RISK MONITORING

So far we have been confronted with two terms **GOVERNANCE and MANAGEMENT.** So now we will study the key practices of risk management covering the aforesaid terms.

KEY GOVERNANCE PRACTICES OF RISK MANAGEMENT:

(याद रखें यह **GOVERNANCE** करने के लिए तरीके है by the management)

1. Evaluate risk management:
   - -- **Examine and make judgement on effect of risk on current & future use of IT in enterprise.**
   - -- **Examine the enterprise's appetite of the risk & these risks are identified and can be managed.**

2. Direct the risk management:
   - -- **Direct (संचालन) the establishment of risk management practices so as to ensure that actual IT risks don't exceed the board's risk appetite.**

3. Monitor Risk management: (Risk management process की निगरानी):
   - -- **Monitor the goals of the risk management processes.**
   - -- **And establish how deviations are identified, tracked and reported.**

KEY MANAGEMENT PRACTICES OF RISK MANAGEMENT:

(याद रखें यह **RISK MANAGE** करने के STEPS है)

CODE TO REMEMBER: **DAM-EAR^2**

1. Data Collection:
   -- **Identify and collect relevant data to ensure effective IT related risk identification, analysis & reporting.**

2. Analyse Risk:
   -- **Develop useful information to support risk decisions.**

3. Maintain the risk profile:
   -- **Make list of the known risks and risk attributes.**
   -- **For instance-** frequency, potential impact, responses and current control activities.

4. Articulate(to say something) Risk:
   -- **Provide information on current state of IT related exposures and opportunities on time to all stakeholders' for appropriate response and action.**

5. Risk management action portfolio:
   -- **Manage opportunities and reduce risks to acceptable level.**

6. Respond to Risk:
   -- **Respond in timely manner so as to limit the magnitude of the loss from IT related events.**

CA AKHIL MITTAL

8. IT COMPLIANCE REVIEW :

To ensure effective ERM (Enterprise Risk Management), the regulators feels the need to mandate its enforcement to comply with **governance, risk management & compliance. (GRC)**

Effective ERM implementation needs various drivers or factors such as:
1. Holistic approach (encompasses entity from top-down)
2.Best practices framework.
3.Technology deployment.
4.Regulatory requirements.

COMPLIANCES IN COBIT 5 :

The MANAGEMENT Monitor, Evaluate and Assess domain contains a compliance focused process:

MEA03 Monitor, evaluate and assess compliance with external requirements.

PROCESS DESCRIPTION	PROCESS PURPOSE
Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.	Ensure that the enterprise is compliant with all applicable external requirements.

Some of the compliances in COBIT 5:

1. It has to be ensured that MEA03 (compliance with external regulatory requirements) complied with but also of the enterprise governance determined policies, procedures and principles.
2. COBIT 5 suggests accountabilities and responsibilities for enterprises roles and governance structure for each process.
3. COBIT 5 frameworks include necessary guidelines to support GRC objectives and supporting activities.
4. COBIT has a specific focus on compliance activities within the framework and explains how they fit within the enterprise picture.

KEY MANAGEMENT PRACTICES OF IT COMPLIANCE:

COBIT 5 provides key management practices for ensuring compliance with the external compliances. Following are the practices:

1. **Identify external compliance requirement: (compliance की पहचान करना)**

   -- Identify and monitor the changes in local and international rules and regulations that have to comply from IT perspective.

CA AKHIL MITTAL

2. **Optimise response to external requirements:(legal requirements के अनुसार नीतियों को adjust करना)**

   --Review and adjust policies, procedures, methodologies so as to sure that legal, regulatory and contractual requirements are addressed and communicated.

   --Consider the industry standards and codes of good practices.

3. **Confirm external compliances:**

   --Confirm the policies, procedures, standards, principles with the external legal, contractual and regulatory requirements.

4. **Obtain assurance of external compliances:**

   -- obtain the report of assurance of compliances and adherences with policies, procedures.

KEY METRICS FOR ASESSING COMPLIANCE PROCESS:

Sample metrics for reviewing process of evaluation and assessing compliances:

COMPLIANCE WITH EXTERNAL LAWS

1. Cost of non-compliance (fines etc)
2. Number of IT related issues reported to the board.
3. Number of non-compliance related to contractual agreement with IT service providers.
4. Coverage of compliance assessments.

IT COMPLIANCE WITH INTERNAL POLICIES

1. Report of non-compliance of policy.
2. Percentage of stakeholders who understand policies.
3. Frequency of policies review and updates

9. COBIT 5 – A GEIT FRAMEWORK :

As per COBIT, information is the success drivers but also it can't be ignored that it also raises governance and management issues too. This section explains need for using approach and latest thinking for reviewing and implementing governance and management of enterprise IT.

Following are the benefits of COBIT 5:

1. Allows IT to be governed and managed in a holistic manner for the entire enterprises.
2. It helps to manage IT related risks and ensure compliances, continuity, security and privacy.
3. It is useful for all types or sizes of the enterprises.

NEED FOR ENTERPRISES TO USE COBIT 5:

-- Enterprise needs good, reliable, repeatable data on which they can take good business decision.

-- COBIT 5 is made and is customised to suit all the enterprises irrespective of their size, industries and geographical areas

-- COBIT 5 provides enterprises a tool necessary to understand, utilise, implement and direct important IT related activities.

-- COBIT 5 is intended to deliver business benefits to enterprises:

-- Increased use of IT experts, user satisfaction, less IT related risks etc.

-- Development of IT related business solutions.

-- Increased enterprise wide involvement in IT related activities.

INTEGRATING COBIT WITH OTHER FRAMEWORKS:

It is based on an enterprise view and is aligned with governance best practices. COBIT 5 acts as the single framework, which serves as a consistent and integrated source of guidance.

- **GEIT**
  This fourth edition of the IT Governance Institute's status report of the governance of enterprise IT covers 21 countries and 10 industries. It reveals accord on the contribution of IT to business success, the challenges and opportunities connected with IT the impact of the economic crisis and views on IT outsourcing, social networking.

- **ITIL**
  The **Information Technology Infrastructure Library** (**ITIL**) is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business

- **TOGAF**
  The Open Group Architecture Framework (TOGAF) is a high level and holistic approach to design, which is modelled at four levels: **Business, Application, Data, and Technology**. It aims at giving a well-tested overall starting model to information architects, which can then be built upon. It relies heavily on modularization, standardization and already existing, proven technologies and products.

- **ISO 27000**
  The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS). It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, and then implement appropriate information security controls according to their needs

***IMP:* No need to remember the explanation to above said best practices.**

CA AKHIL MITTAL

COMPONENTS OF COBIT:

COMPONENTS	DESCRIPTION
FRAMEWORK	Organise IT governance objectives and good practices by IT domains and processes and links to business requirement.
PROCESS DESCRIPTION	Common language for everyone in the entity. The processes map to responsibilities areas of plan, build, run and monitor.
CONTROL OBEJCTIVES	Provide comprehensive requirements to be considered by the management for effective control for the processes.
MANAGEMENT GUIDELINES	Helps in assigning responsibilities, agree on objective, measure performance.
MATURITY MODEL	Organise IT governance objectives and good practices by IT domains and processes.

BENEFITS OF COBIT 5:

I am categorizing the benefits in to 3 parts:

IT RELATED BENEFITS:

1. COBIT 5 helps in managing IT related risks and ensure compliances, security and privacy.
2. COBIT 5 enables in providing clear development and good practices for IT management.

ENTITY GOALS AND IT:

1. COBIT 5 enables enterprises in achieving their objectives for governance and management of enterprise IT.
2. COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realizing benefits and optimizing risks level and resource use.
3. COBIT 5 enables IT to be governed in such a manner that to ensure full end-to-end business and IT functional areas of responsibilities, considering the interest of internal and external stakeholders.

GENERAL BENEFITS:

1. COBIT 5 supports compliance with relevant laws, regulations, agreements and policies.
2. COBIT 5 is useful for all types of organization whether commercial or not.

CUSTOMISING COBIT AS PER NEEDS:

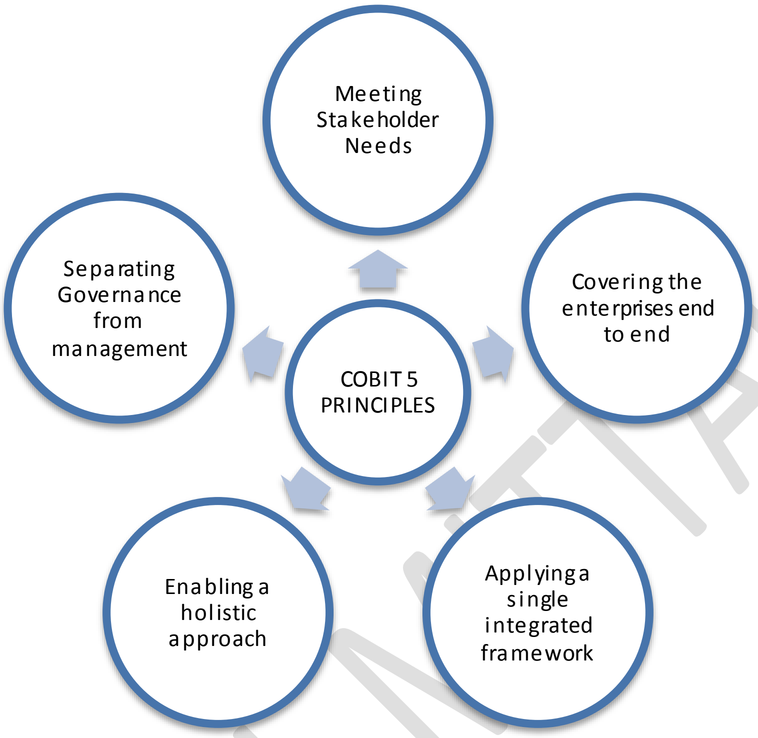
COBIT 5 can be tailored to meet the enterprise's need. Because of its open design, it can be applied to meet needs related to:

-- Information security
-- Risk Management
-- Financial Processing
-- Assurance Activities
-- Governance & Management of enterprise IT
-- Legislative & regulatory compliance

CA AKHIL MITTAL

FIVE PRINCIPLES OF COBIT:

There are 5 key principles for governance & management of enterprise IT.


Meeting Stakeholder Needs
Covering the enterprises end to end
Applying a single integrated framework
Enabling a holistic approach
Separating Governance from management
COBIT 5 PRINCIPLES

CA AKHIL MITTAL

Now explaining each of the steps in detail:

1. Meeting Stakeholder Needs:

-- Enterprise exists to create value for their stakeholders, by maintaining balance,

-- Between **benefit realisation** & **risk optimisation.**

-- COBIT 5 enables the enterprises to create such value by using COBIT processes.

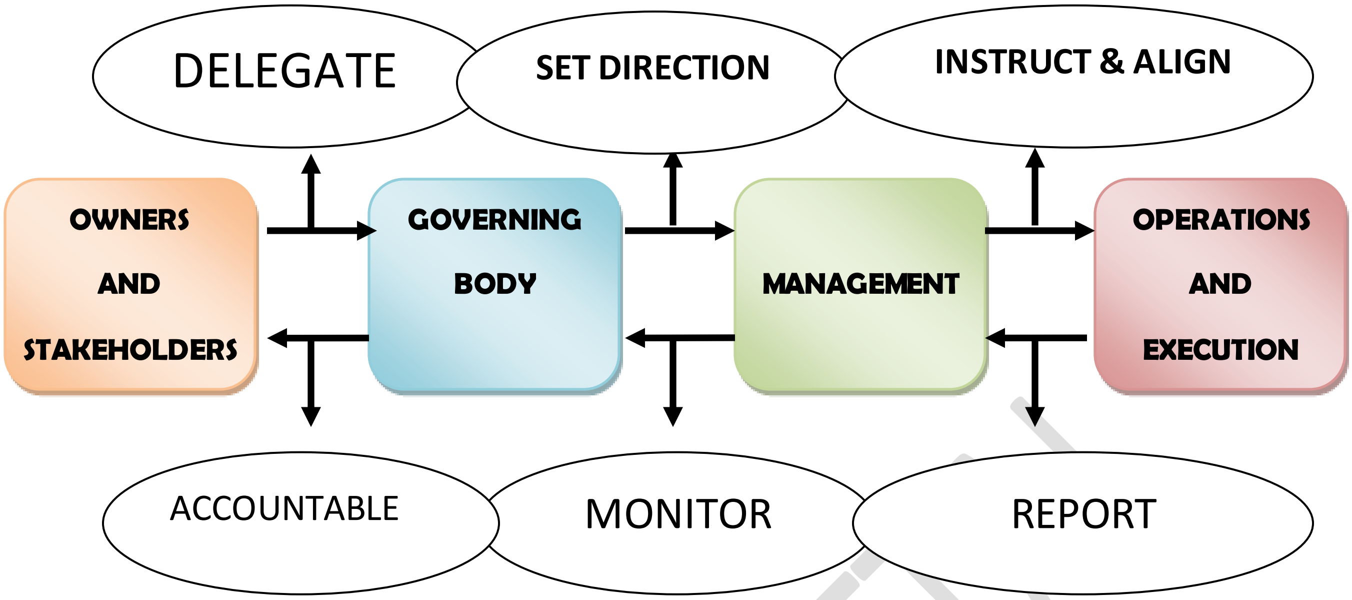
-- Since it is tailor made, as such an enterprise can easily modify it as per its requirement.

2. Covering enterprise End-to-End:

-- It covers all functions & processes within the enterprise.

-- COBIT 5 doesn't focus on IT function but treats information as an asset that need to be dealt with just like any other asset.

-- It considers all in the enterprise whether internal or external that is relevant to governance & management of enterprise information and related IT.



3. Applying a single Integrated Framework:

-- Since COBIT 5 can be integrated with other standards & frameworks,

-- It is a single integrated framework that enables complete company coverage, providing a basis to integrate effectively other frameworks.

4. Enabling a holistic(Relating to or concerned with wholes or complete systems **) approach:**

-- Effective governance of enterprise IT requires holistic approach.

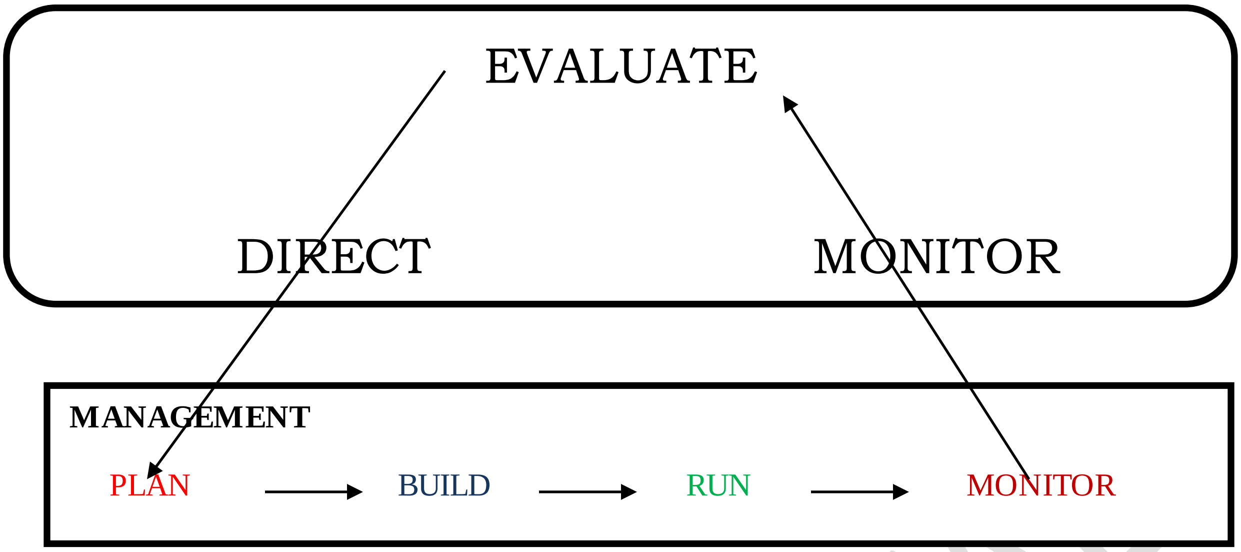
-- COBIT 5 defines a set of enablers to support the implementation of governance and management system for enterprise IT.

5. Separating Governance from management:

-- COBIT 5 makes a clear distinction between governance & management.

GOVERNANCE	Ensures that stakeholder needs, conditions & options are evaluated to determine BALANCED, objectives to be achieved, setting direction, through decision making & monitoring. GOVERNANCE is responsibility of the BOARD OF DIRECTORS under the CHAIRPERSON.
MANAGEMENT	Plans, builds, run and monitor activities in alignment with the direction set by the governance body to achieve organisational objectives.

CA AKHIL MITTAL



COBIT 5 ENABLERS MODEL:

COBIT 5 is the successor of the COBIT 4.1 process model, incorporating both RISK IT and VAT IT framework. COBIT 5 enabler model comprises of 37 governance and management processes:

GOVERNANCE PROCESSES:

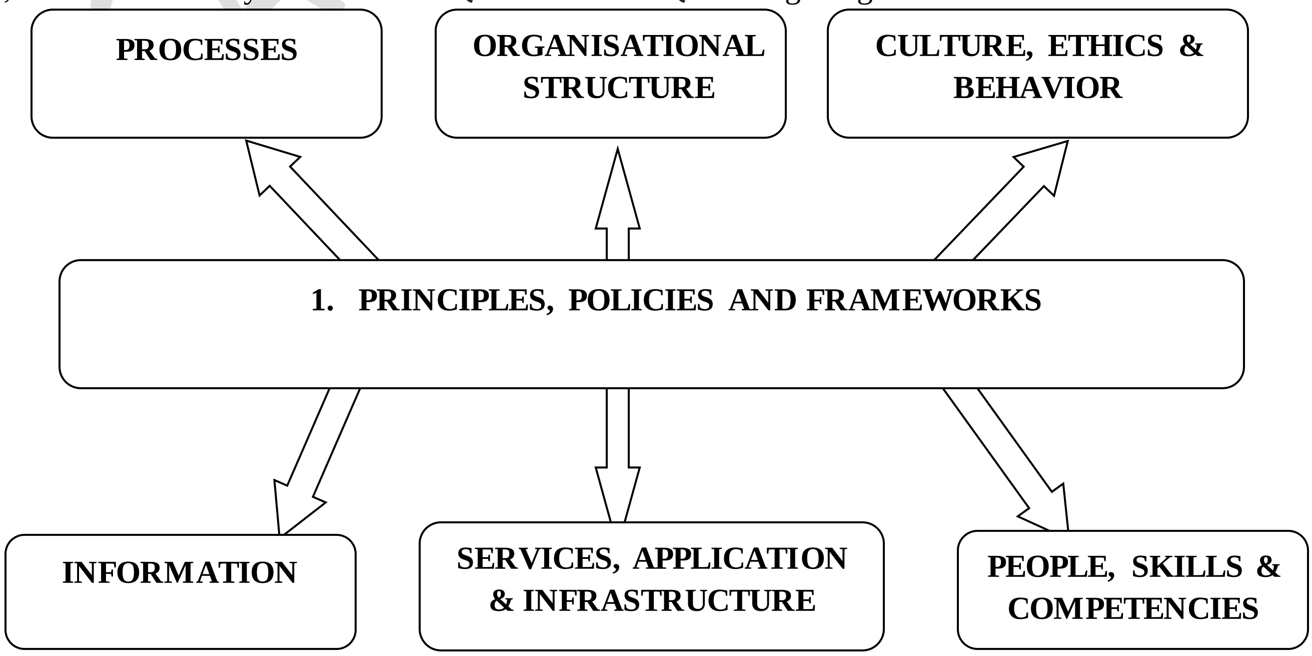
- Evaluate, direct and monitor practices (EDM) – 5 processes (EDM01 to EDM05)

MANAGEMENT PROCESSES:

- Align, plan and organise(APO) – 13 processes (APO01 to APO13)
- Build, acquire and Implement (BAI) – 10 processes (BAI01 to BAI10)
- Deliver, service and Support (DSS) – 6 processes (DSS01 to DSS06)
- Monitor, Evaluate and Assess (MEA) – 3 processes (MEA01 to MEA03)

COBIT 5 ENABLERS:

Enablers are the factors **that collectively and individually influence** whether something **will work. Enablers** are driven by the **GOALS.** The COBIT 5 framework describes **7** categories of the enablers. **In** Hindi, I would rather say factors ko क्या हासिल करना चाहिए for a good governance.


PROCESSES
ORGANISATIONAL STRUCTURE
CULTURE, ETHICS & BEHAVIOR
1. PRINCIPLES, POLICIES AND FRAMEWORKS
INFORMATION
SERVICES, APPLICATION & INFRASTRUCTURE
PEOPLE, SKILLS & COMPETENCIES

CA AKHIL MITTAL

To remember: In **organisation structure** there are **people with skill & competencies that** use **information** to introduce **principles, policies & framework** in the processes so that there exist good **culture, ethics & behaviour.** After all this, company can provide quality **services, infrastructure & applications.**

1.Organisational Structure: This is the key **decision making** entities in the enterprises.

2.People with skill & competencies: All this required for successful completion of all activities and for making correct decision.

3. Information: It is needed at all level of management. It is required to keep organisation running and well governed.

4. Principles, policies & framework: These are the vehicle to translate desired goals into practical guide for day-to-day operations.

5.Culture, ethics & behaviour: Of individuals & enterprises is important part for the governance & management activities.

6.Services, infrastructure & applications: This provides company information technology processing and services.

COBIT 5 PROCESS REFERENCE:

COBIT 5 includes a process reference that describes in detail **a number of governance and management processes.** Characteristics:

-- It represents all processes normally found in the enterprise IRO IT activities.

-- Proposed process model is **complete, comprehensive model.**

-- Each enterprise has different processes to achieve common goals.

-- Good governance depends on **common language** usage for all parts of enterprise involved in **IT activities.**

USING COBIT 5 BEST PRACTICES FOR GRC (governance, risk management & compliance):

GRC primarily aimed towards compliances of legal requirements, it is advisable to consider business requirements so as to optimise the investment in implementing the IT resources.

GRC program implementation requires:

1.GRC requirements are applicable.
2.Identify regulatory and compliance scope.
3.Current GRC current status.
4.Setting out the parameters/standards on which success will be measured.
5.Adapt best global practices.
6.Using auditable standard approaches.

Following are the important points in respect of COBIT 5 and GRC:

1.It is responsibility of management to ensure proper implementation and monitoring of GRC measures.

CA AKHIL MITTAL

2.GRC helps in meeting external compliances as well as fulfil business requirements.
3.COBIT 5 helps in discharging the responsibilities by ensuring that all aspects of GRC are implemented.
4.It is advisable for the enterprise to adapt mandatory GEIT (Governance of Enterprise IT).

Success of a GRC program can be measured by using the following goals and metrics:
(GRC कार्यक्रम की सफलता के क्या लक्षण है)

1.**Less time in executing the controls.**
2.Reduction in **TIME** required in **CONDUCTING THE AUDIT** for key business areas.

3.**Reduction of expenses** in relation to legal, regulatory and review areas.
4.**Timely reporting of** regular compliance issues and remedies.

10. INFORMATION SYSTEM ASSURANCE :

In this rapid and inter-linked business scenario, it is imperative for the business to critically and effectively govern the information and related technologies.

As a result the management is under tremendous pressure to ensure effective use of the information and technology and IT related investments.

So there begins new challenges for the CHARTERED ACCOUNTANTS to cope up with the changing environment and provide **assurance with required level of confidence.**

USING COBIT 5 for IS assurance:

Auditors have to understand the business processes and also the business policies and procedures as implemented.

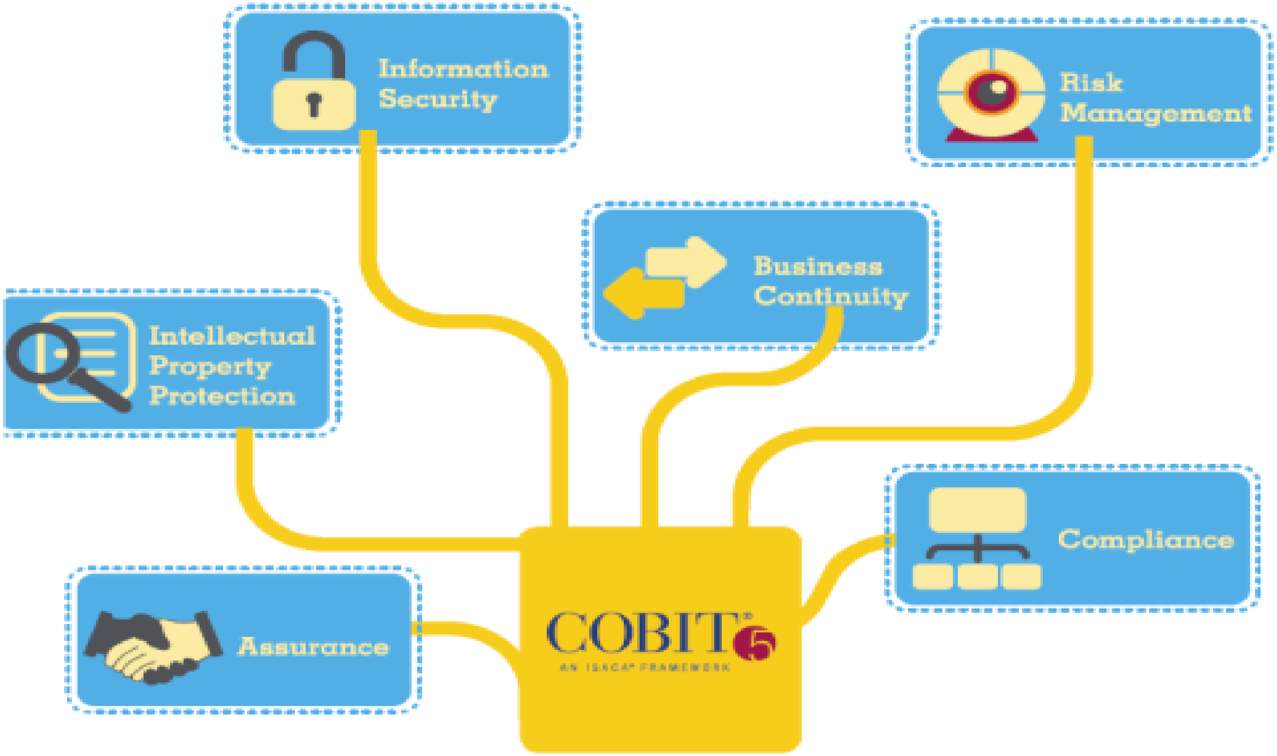
Also management execute its business through staff and thus it is required that **staff have defined job responsibilities.**

The organization structure needs to have internal control structure. IT impacts the way business operations could be performed and internal controls are implemented. Auditor must know the organization structure.

CA AKHIL MITTAL

COBIT 5 importance's in business:

1. Engineered to meet the expectations of multiple stakeholder (External & internal Stakeholders).
2. External Stakeholders: **Customers, business partners:** Internal Stakeholders: **Board, employees etc.**
3. It is non-technical language and hence can be understood by the management too.



CA

EVALUATING IT GOVERNANCE STRUCTURE AND PRACTICES BY INTERNAL AUDITORS:

IT governance can be evaluated by both internal and external auditor. However, **Institute of Internal Auditor (IIA)** issues guidance on internal audit. Features of guidelines:

1. Relates to governance structure and practices which are subject to internal audit.
2. Following are the key components that lead to effective IT governance : (auditor को क्या verify करना है)

   a. Leadership:

   -- There must be synchronization between IT objectives and business needs. Auditor must evaluate the ability of leadership to effectively communicate the nexus between the two to IT & organizational personnel.

   -- Evaluate the leaders' involvement in development & execution of entity strategic goals.

   -- Review how roles & responsibilities are assigned within IT organization.

   -- Review the role of senior management in maintaining of strong IT governance.

   b. Organizational structure:

   -- Evaluate how management & IT personnel are interacting and communicating needs of entity.

   -- This should include existence of roles and reporting relationships to allow IT to meet needs of the organization.

c. **Processes:**

-- Evaluate IT process activities, and controls in place to mitigate risks to the organization.

-- Evaluate processes that are used by IT organization to support IT environment & consistent delivery of the services.

d. **Risks:**

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

-- Determine the accountability of the personnel within the risk management.

e. **Controls:**

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

-- Ownership, documentation and reporting of self validation aspects.

-- Controls must be strong enough to address the identified risks based on the organization's appetite for the risks.

f. **Performance measurement:**

-- Evaluate the framework and systems in place to measure the organizational outcomes where IT plays an important role in business operations.

SAMPLE AREAS OF GRC FOR REVIEW BY INTERNAL AUDITORS:

Institute of Internal Auditor (IIA) provides areas which have to be reviewed by internal auditor as part of review of governance**, risk management & compliance. (GRC) areas:**

A. SCOPE:

-- Internal audit activities must evaluate and contribute to improvement in governance, risk management and control processes by using approaches.

B. GOVERNANCE:

The internal audit must assess and make recommendations for improving the governance process for the following objectives:

-- Performance of organizational to be ensured.

-- Ethics promotion within the organization.

-- Activities coordination and communication among management and auditors.

-- Risk Communication and control information to required areas of organization.

C. EVALUATE ENTERPRISE ETHICS:

-- Auditor must evaluate **design, effectiveness and implementation** of organization's ethics programs, activities.

-- Auditor must evaluate whether IT governance supports organization's strategies & objectives.

D. RISK MANAGEMENT:

-- Auditor must evaluate **effectiveness and management's contribution in improvement in the risk management processes.**

CA AKHIL MITTAL

E. INTERPRETATION:

-- Determine whether risk management processes are in place and effective in operations. Auditor must examine and evaluate that:

1. Significant risks are identified. **2. Appropriate risks response identified that aligns with risk appetite.**
3. Relevant risk information is captured and communicated to the all levels of the management.

F. RISK MANAGEMENT PROCESS:

-- Auditor must gather information to support the assessment of risk management processes during multiple engagements.

-- When all engagements taken together provide comprehensive understanding of organization's risk and management processes and their effectiveness.

G. EVALUATE RISK EXPOSURES:

-- Auditor must evaluate risk exposures relating to organizations governance, operations & information system regarding:

-- <u>**C**</u>ompliances with laws, regulations, policies etc.
-- <u>**A**</u>sset safeguarding
-- <u>**R**</u>eliability and integrity of financial information.
-- <u>**O**</u>rganization's objectives accomplishment.

CODE TO REMEMEBER: **C.A.R.O**

(Just like in CARO (AUDIT) auditor is responsible to provide assurance)

H. EVALUATE FRAUD AND FRAUD RISKS:

-- Auditor must evaluate potential for occurrence of fraud & how organization manages fraud risks.

I. ADDRESS ADEQUACY OF RISK MANAGEMENT PROCESS:

-- Auditor must incorporate knowledge of risks gained from consulting engagements into their evaluation of organization's risk management processes.

<u>SAMPLE AREAS OF REVIEW OF ASSESSING AND MANAGING RISKS:</u>

-- Review covers **CONTROLS over the IT process of assessing and managing risks**.
(जोखिम को assess करना और manage के प्रक्रिया पर नियंत्रण का review)

-- Controls over risks must assure to management that enterprise all relevant risks as relevant to IT implementation.

-- Generally the review considers whether the entity is engaging itself in risk-identification, impact analysis, taking cost effective measures to mitigate the risks.

-- Some specific areas of evaluation are:

-- Risk management ownership & accountability. **(Risk management में accountability fix** करना)
-- Different kinds of IT risks. **(अलग types के risk** को evaluate करना)
-- Root cause analysis & mitigation measures. **(Risk के कारण की पहचान & उपाय)**
-- Defined and communicated risk tolerance profile. **(Risk** को communicate करना)
-- Risk assessment methodologies and action plan and reassessment.

CA AKHIL MITTAL

EVALUATING AND ASSESSING THE SYSTEM OF INTERNAL CONTROL :

COBIT 5 has specific process: **MEA02 Monitor, Evaluate and assess the system of internal control.**
-- Provide guidelines on evaluating and assessing internal controls implemented in an enterprise.

This review includes:

-- Plan, organize and maintain standards for internal controls assessment. **(Set the standards)**
-- Enable management to identify deficiencies and inefficiencies. **(Search deficiencies)**
-- Continuously monitor and evaluate control environment. **(Monitoring of internal controls)**

There are some key practices for assessing and evaluating the internal control system:
(I am for the sake of learning dividing the points in the following manner)

PART A : MONITORING ASPECTS	
MONITORING OF:	
-- Internal Controls	Continuously monitor benchmark and improve IT control environment in order to meet the organizational needs.
-- Business Process Efficiency	Following things are covered under this review of internal control: --**Review operation of controls** (How controls work in entity) --**Review of monitoring & test evidences to ensure controls are effectively operating.** --**Maintain of evidences such as per periodic testing of controls, independent assessment etc.**
-- Report Control deficiencies	--Identify deficiencies in controls and analyze the root cause of such deficiencies. --Report such deficiencies to the stakeholders.
-- Perform Control self-assessment	--Encourage management to take positive ownership of control improvement through continuous program of self-assessment.

PART PART B : INITIATIVE ASPECTS	
-- Plan Assurance Initiatives	-- Plan assurance initiative based on enterprise objectives, -- Assurance objectives, strategy priorities, inherent risk resource constraint
-- Scope Assurance Initiatives	--Define and agree with management on scope of assurance initiative based on assurance objectives.
-- Execute Assurance Initiatives	--Execute planned assurance initiatives. --prepare report on identified findings. --Provide assurance opinions, recommendation for improvements related to operational performance, external compliance & internal controls.

CA AKHIL MITTAL