# CG = Corporate Governance
FRS = Financial Reporting Standard

Date :
Page No.

CONCEPT of

GOVERNANCE AND MIS

1. Basics :-

GOVERNANCE → ENTERPRISE GOVERNANCE

(i) Derived from Greek word meaning "to steer"

(ii) All processes of governing whether undertaken by

Government market network

Over a family, tribe, formal or informal organisation or territory

AND

whether through laws, norms, power or language.

(iii) All means and mechanism that will enable multiple stakeholders of an enterprise to

Assess or evaluate → setting → monitoring

options in an organised direction compliance & performance.

manner

To satisfy specific Enterprise objectives.

(i) set of responsibilities & practices

↓

... exercised by board and executive management for

↓ Board is at strategic level, so, dis ↑ word is used.

providing strategic direction achievement of objective, ascertaining risk and managing appropriately and verifying organisation resources are used responsibly.

↓

Ex- Code on CG and FRS.

monitored by Audit committee.

It is Boards responsibility, with no dedicated oversight mechanism

ENTERPRISE GOVERNANCE.

(IT Governance and CG are same in terms of obj)

CORPORATE GOVERNANCE (IT Governance)

(i) Also known as conformance.

(ii) A system by which activities of a company or enterprise is directed and controlled

↓

to achieve objective of increasing shareholder value (ultimate objective)

↓

by enhancing economic performance (business objective)

(iii) Ex – Sarbanes Oxley Act of US and clause 49

BUSINESS GOVERNANCE

(i) Also known as Performance.

(ii) A pro-active approach

(iii) Business oriented & forward looking view

(iv) Focuses on strategy and value creation with objective of helping the board to make strategic decisions, understand its risk appetite and key performance drivers

Date:
Page No.

Date :
Page No.

BENEFITS OF GOVERNANCE.

(i) Achieving enterprise objectives
↓
by ensuring that each element of the mission and strategy are
↓
assigned and managed with a clearly understood and transparent decisions rights and accountability framework.

(ii) Defining and encouraging desirable
↓
behaviours in the
↓
use of IT and in the
↓
execution of IT outsourcing arrangement.

(iii) Implementing and integrating the desired business processes into the enterprise.

(iv) providing stability and overcoming the limitations of organisational structure.

(v) A holistic IT governance framework for reducing internal territorial strife and improved relations by
↓
formally integrating the customers, business units and external IT providers in it.

Date :
Page No.

BASIS	IT GOVERNANCE	GOVERNANCE OF ENTERPRISE IT.
SCOPE	narrow ; micro	Broader ; macro.
OBJECTIVE	To determine and cause the desired behavior and results to achieve the strategic impact of IT	Analyse 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 enterprises mission, goals and objectives.
BENEFITS	• Increased value delivered through enterprise IT • Increased user satisfaction with IT services. • Better cost performance of IT • more optimal utilization of IT resources. • Improved agility in supporting business needs.	• A consistent Approach, integrated and aligned with enterprises governance approach. • ensures IT related decisions are made in line with enterprise's strategies and objectives • ensures IT related processes are overseen effectively and transparently. • confirms compliance with legal and regulatory requirement

- Ensures that the Governance requirements for board members are met.

KEY PRACTISES

- Evaluate the Governance system :
  ↳ continually identify and engage with its stakeholders
  ↓
  document an understanding of the requirements
  ↓
  make judgement on the current and future design of Governance.

- Direct the Governance system :
  ↳ Inform leadership and obtain their support, buy-in and commitment
  ↓
  Guide the structures, processes and practises in line with agreed Governance design principles, decision making models and authority level
  ↓
  Define info required for informed decision making.

- monitor the Governance system :
  ↳ its effectiveness and performance.
  ↓
  Provide appropriate oversight of IT

Best Practises of Corporate Governance

→ clear assignment of responsibilities and decision-making authorities, incorporating an hierarchy of required approvals from individuals to the Board of directors.

→ Establishment of a mechanism for the interaction and cooperation among the Board, senior management & auditors.

→ Implementing strong internal control system

→ special monitoring of risk exposures, where conflicts of interest are likely to be particularly great.

→ Financial and managerial incentives to act in an appropriate manner.

→ App info flow internally and to the public.

SOX have used COSO (committee of sponsoring organization) as one of the important guides for implementing Risk management and internal controls

As per executive summary of ERM — Integrated framework published by COSO of Treadway committee highlights the need for management to implement

Date :
Page No.

ENTERPRISE RISK MANAGEMENT

a. system of risk management at the enterprise level.

→ Defination : It is a process, effected by an entity's BOD, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may effect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

↓

ERM deals with risks and opportunity affecting value creation or preservation.

↓

Regulations require enterprises to adopt a risk management strategy (RMS), which is appropriate for the enterprise

↓

Hence, the types of controls implement in IS is depends upon enterprise RMS.

↓

IT security & control are sub-set of risk management strategy.

↓

ERM considers overall objective, processes, organisation structure, technology deployed and risk appetite.

↓

Sarbanes Oxley Act (SOX) in the US → focuses on the implementation and review of internal controls as relating to financial Audit, highlights the importance of evaluating the risks, security and controls as related to F.S.

Responsibility of maintaining IC under SOX → CEOs and CFOs are personally and criminally liable for the quality and effectiveness of organisations IC.

(#IC = Internal control).

Date:
Page No.

Asset safeguarding, system efficiency

data reliability

Internal Controls.

↳ and system effectiveness.

Provide reasonable assurance not absolute assurance

- The US security and Exchange Comission (SEC's) defines Internal control over financial reporting as :-

(Final rules ke andar, ata hain SEC's ka).

↳ A process designed by, or under the supervision of the company's principal executive and principal officers of finance or persons performing similar functions and effected by the company's BOD, management and other personnel to provide reasonable assurance regarding the reliability of financial reporting and preparation of financial statements for external purposes in accordance with GAAP.

Includes policies and procedures that :-

→ maintain records → giving reasonable details → and accurately and fairly reflect → transactions and dispositions of the assets of the company.

→ Providing reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements as per GAAP → all receipts & expenditures of the company are being made only in accordance with authorization of management and directors of the company.

→ Provide reasonable assurance → regarding prevention or timely detection → unauthorised assets transactions → that could have material effect on the financial statements.

Page No.

As per final rules :-

A company's Annual report must include

IC over FR board → evaluate → evaluation reporting → external party attestation ya survey of IC over FR existence

AN INTERNAL CONTROL REPORT OF MANAGEMENT.

A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.

(At end of the company's most recent fiscal year, including a statement as to whether or not the co's internal control over FR is effective)

A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the company's internal control over financial reporting.

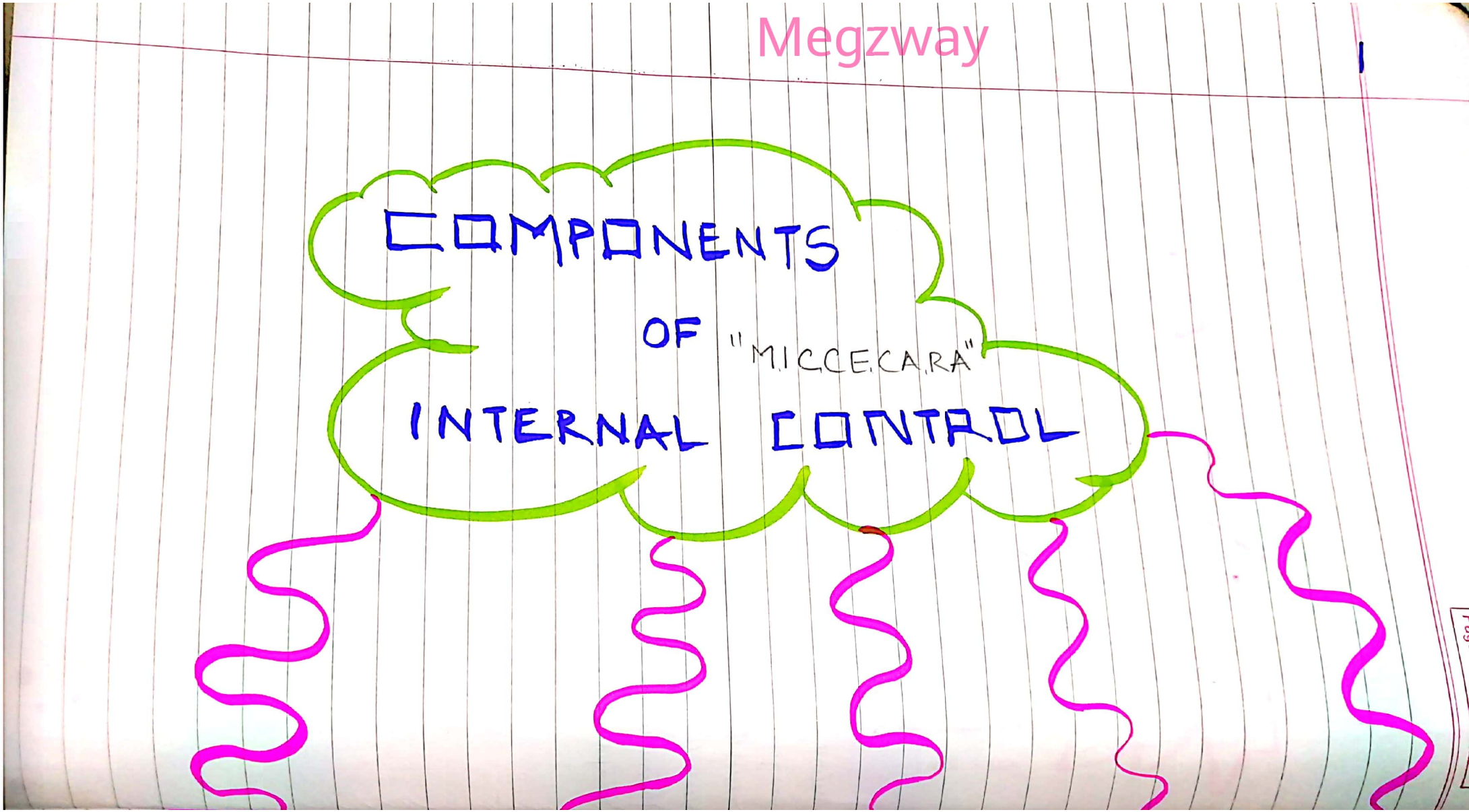
A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.

Disclosure of any "material weakness" in the company's internal control over FR identified by management.

↓

management not permitted to conclude IC over FR as effective if there are one or more material weakness in it.

Megzway



CONTROL ENVIRONMENT (CE)

→ Includes elements that establishes the control context in which specific accounting systems and control procedures must operate

→ It is manifested in
- management's operating style
- the ways authority and responsibility are assigned
- functional method of the audit committee,
- methods used to plan and monitor performance etc.

→ For each business process, org^n should develop and maintain a control environment.

RISK ASSESSMENT (RA)

→ Includes the elements that identify and analyse the risks faced by an organisation and way the risk can be managed

→ A control environment must include RA associated with each Business process, so that material loss risk can be identified and managed

CONTROL ACTIVITIES (CA)

→ Includes the elements that operate to ensure transactions are authorised, 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)

→ CA must be developed to manage, mitigate & reduce risks associated with each business process

INFORMATION AND COMMUNICATION (IC)

→ 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.

→ Associated with CA

→ Enables organisation to capture and exchange info needed to conduct, manage and control its business processes.

MONITORING (M)

→ IC process must be continuously monitored with modifications made as warranted by changing conditions.

→ Ensures IC operates reliably over time.

Date :
Page No.

managerial processes are :- (•) planning (•) reporting
(•) organising (•) Budgeting
(•) staffing
(•) directing
(•) coordinating

Date :
Page No.

Business and IT Strategy.

management strategy determines at the macro level the path and methodology of rendering services by an enterprise

↓

It outlines the approach of the enterprise

↓

formulated by senior management

↓

based on such strategy adapted, relevant policies and procedures are formulated.

↓

From business strategy perspective, IT is affecting the way in enterprises are structured, managed and operated

↓

one of the most dramatic developments affecting enterprise is the fusion of IT with business strategy.

↓

Enterprise can no longer develop business strategy separate from IT strategy and vice-versa.

↓

Sound IT planning + business planning + effective financial and management controls within new systems.

↓

Every Enterprise regardless of its size needs to have an internal control system built into its enterprise structure

↓

Date :
Page No.

Auditors may also be required to provide consulting before, during or after implementation of information systems strategy

↓

hence, they are required to have a good understanding of management aspects as relevant to deployment of IT and IT strategy, which includes understanding IS strategy, policies, procedures, practises and enterprise structures, segregation of duties etc.

↓

IT organisations should define their strategies and tactics to support the organisation by ensuring that day-to-day IT operations are delivered efficiently and without compromise.

↓

metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices.

→ Internal audit can determine whether the linkage of IT metrics and objectives aligns with organisation's goals, regularly measured progress of IT and express an opinion on whether the metrics are relevant and useful

Date :
Page No.

IT Steering Committee.

* 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 steering committee.

Depending on size and needs of the enterprise, senior management may appoint a high level committee to provide appropriate direction to IT deployment and IS and to ensure that the IT deployment is in line with enterprise business goals and objectives.

This committee is called IT steering committee.

- Led by a member of BOD
- It role and responsibility must be documented and approved by senior management.
- comprises of functional heads from all key departments of the enterprise including audit and IT department, who are responsible for taking decisions relating to their departments as required.

* KEY FUNCTIONS OF COMMITTEE INCLUDES:-

Ensure that long + short range plans of IT department in tune with enterprise goals and objectives.

Establish size and scope of IT functions and set priorities within the scope.

Review and approve major IT deployment projects in all their stages

Review the status of IS plans, budgets and overall IT performance.

Review and approve standards, policies and procedures.

Facilitate implementation of IT security within enterprise

Report to the BOD on IT activities on a regular basis.

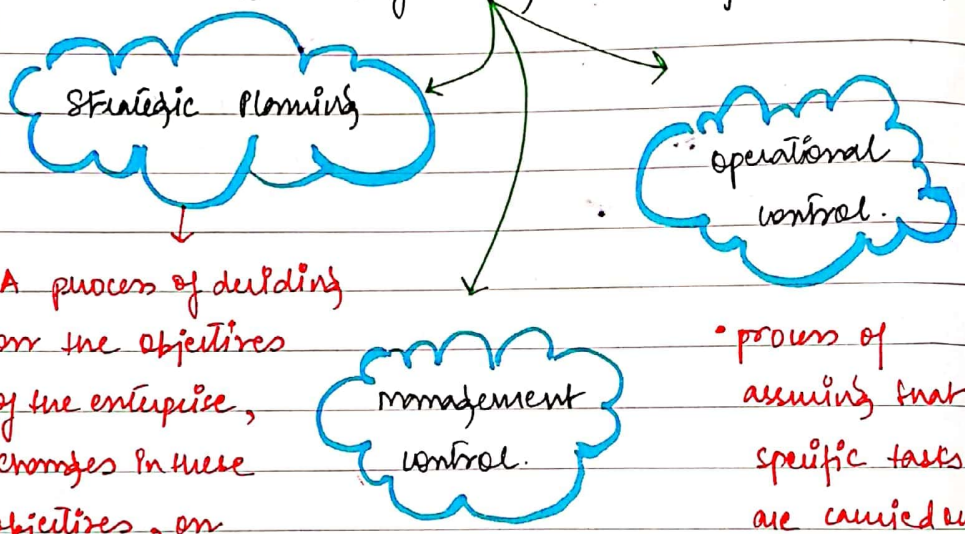
Corporate-level strategic planning is the process of determining the overall character, purpose of organization business it will enter and leave & how resources will be distributed among those businesses.

Date :
Page No.

IT Strategy Planning

Basically deciding in Advance.
→ what is to be done. ?
→ who is going to do ?
→ when it is going to be done ?

There are three levels of managerial activity in an enterprise



- A process of deciding on the objectives of the enterprise, 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.
- Done by Top management

- A process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the enterprise's objective.

- process of assuring that specific tasks are carried out effectively and efficiently.

Date :
Page No.

IT strategic plans provide direction to deployment of IS and it is important that key functionaries in the enterprise are aware and are involved in its development and implementation.

↓

management should ensure that IT long and short range plans are communicated to business process owners and other relevant parties across the enterprise

↓

management should establish processes to capture and report feedback from business process owners and users regarding quality and usefulness of long and short range plans of IT

↓

Feedback obtained should be evaluated and considered in future IT planning.

Date :
Page No.

IT strategic planning process:

→ Has to be dynamic in nature
→ A process by which IT management and business process owners ensure to modify IT long range plans in a timely and accurate manner to accommodate changes to the enterprise's long range plans and changes in IT conditions
→ IT long range plans is regularly translated into IT short range plans
→ IT short range plans ensure IT functional resources are allocated on a basic consistent with IT long range plans.
→ IT SRP should be reassessed periodically and amended as necessary to response to changing business and IT conditions

Date :
Page No.

CLASSIFICATION OF "STRATEGIC PLANNING"

→ Planning undertaken by top management towards meeting long-term objectives of the enterprise.

IT STRATEGIC PLANNING

Enterprise strategic Plan.

→ Business planning determines the overall plans of the enterprise, overall character.

→ primary plans prepared by top management that guides the long run development of the enterprise.

→ Includes a statement of mission, specification of strategic objective, assessment of environment and organisation factors.

IS strategic Plan.

++

Enablers of IS strategic Plan → key enablers are :-

→ Enterprise business strategy.

→ Definition of how IT supports the business objectives.

→ monitoring the technology markets

→ Existing systems Assessment.

IS Requirements Plan

→ It defines IS architectures for the IS department are :-

→ Automated data repository & dictionary.

→ Data syntax rules,

→ Data ownership and criticality / security classification

→ Enterprise IS Architectural standards.

IS Application and facilities Plan.

Date :
Page No.

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

Date :
Page No.

KEY MANAGEMENT PRACTICES FOR ALIGNING IT STRATEGY WITH ENTERPRISE STRATEGY.

- Understand enterprise direction : → current enterprise environment
  → Business processes
  → enterprise strategy
  → future objectives.
  → External environment.
- Assess the current environment, capabilities and performance. : → performance of current internal businesses
  → IT capabilities and external IT services.
  → enterprise architecture in relation to IT.
  → Identify issues currently being experienced and develop improvement recommendation to benefit.
  → potential cost and benefits of using external services.
- Define the target IT capabilities : → define target business, IT capabilities and required IT services.

  on basis of → understanding of enterprise environment
  → Assessment of current business process, IT environment and issues.
  → consideration of reference standards, best practices and validated emerging technologies or innovation proposals.

- Conduct a gap analysis : → Identify the gaps between the current and target environments
  → Consider alignment of assets with business outcomes to optimise investment in and utilization of the internal and external asset base

- Define the strategic plan and road map:
  - How IT will support IT enabled investment programs, business processes, IT services and IT assets.
  - Create a strategic plan that defines, in cooperation with relevant stakeholders, how IT related goals will contribute to enterprise's strategic goals

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

- Communicate the IT strategy and direction:
  → To appropriate stakeholders and users throughout the enterprise.

Date :
Page No.

BUSINESS VALUE FROM USE OF IT.

(Best/effective use)

- It is achieved by ensuring optimisation of the value contribution to business from the business processes, IT services and IT assets resulting from IT-enabled investments at an acceptable cost.

- Key management practices for evaluating BVFUOI are:-

→ Evaluate value optimisation
↓
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

direct value optimisation
↓
direct value management principles and practices to enable optimal value realisation from IT enabled investments throughout their full economic life cycle.

monitor value optimisation.
↓
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.

Date :
Page No.

RISK MANAGEMENT

* Key components of an effective IT governance structure of any enterprise :-
  - → Enterprise Risk Management
  - → IT Risk management.

  } provides linkage between them through activities.

* Risk → Possibility of something adverse happening, resulting in potential loss/exposure.

* Risk management → Process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining the level of risk.

* An Information System based on IT has its inherent risks → These risks cannot be eliminated but they can be mitigated by appropriate security → this security has to be implemented as per required control systems envisaged by the management of the enterprise. → Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate risk. → If controls are unavailable, inadequate or inappropriate, the control weakness has to be reported to auditee management with appropriate recommendations to mitigate them
  → Based on the point of impact of risks, controls are classified.
  - Preventive – Prevent risk from actualising.
  - Detective – Detect the risks as they arise.
  - Corrective – Facilitate correction.

  → Risk in IT environment are mitigated by providing appro –

Date :
Page No.

and adequate IS security. ⟶ IS security is defined as "procedures and practices to assure that computer facilities are available at all required times that data is processed completely and efficiently and that access to data in computer systems is restricted to authorized people".

* Sources of risk :-
  ↓
  Areas from where risks can occur.
  ↓
  It will give info about the possible threats, vulnerabilities and accordingly appro risk mitigation strategy can be adapted.
  - Commercial and legal relationships.
  - Economic circumstances.
  - Human Behavior
  - Natural Events
  - Political circumstances

* Characteristics of risk :-

① Loss potential that exists as the result of threat/vulnerability pairs.

② Uncertainty of loss expressed in terms of probability of such loss; and

③ The probability/likelihood that a threat-agent mounting a specific attack against a particular system.

Date :
Page No.

Important Terms :

ASSET – Something of value to the organisation.

- Info in electronic or physical form
- Software system
- employees

characteristics :-

→ Recognised to be of value to the organisation.

→ not easily replaceable without cost, skill, time, resources or a combination.

→ Part of corporate identity of an organisation, which absence may be a threat for an organisation.

→ their data classification would normally be (•) proprietary
(•) Highly confidential, or
(•) Top secret

THREATS – Any entity, circumstance or event with the potential to harm the assets through its unauthorised access, destruction, modification, and/or denial of service.

- Assets and threats are closely correlated.
  without a threat asset
- Typically prevented by applying some sort of protection to assets.

LIKELIHOOD (of a threat) – Estimation of the probability that the threat will succeed in achieving an undesirable event.

Date :
Page No.

EXPOSURE - 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.

ATTACK - An attempt to gain unauthorized access to the systems services or to compromise the systems dependability.

- A malicious intentional fault, usually external fault with an intent of exploiting vulnerability in the target
- A set of action designed to compromise confidentiality, integrity or availability (CIA) or any other defined feature of an IS.
- An attempt to defeat IS safeguards.

Risk assessment includes :-

→ Identification of threats and vulnerabilities in the system.
→ Potential impact or magnitude of harm that a loss of CIA would have on enterprise operations, assets, if an identified vulnerability is exploited by a threat
→ Identification and analysis of security controls for the IS

Date :
Page No.

Information System can generate many risk (direct and indirect)

↓

This leads to gap between the need to protect system and degree of protection applied.

↓

GAP is caused by :-

- (•) Widespread use of technology
- (•) Interconnectivity of systems.
- (•) Elimination of distance, time and space as constraint
- (•) Unawareness of technological changes.
- (•) Devolution of management and control

COUNTER MEASURE : An Active device procedure technique or other measure that reduces the vulnerability of a component or system.

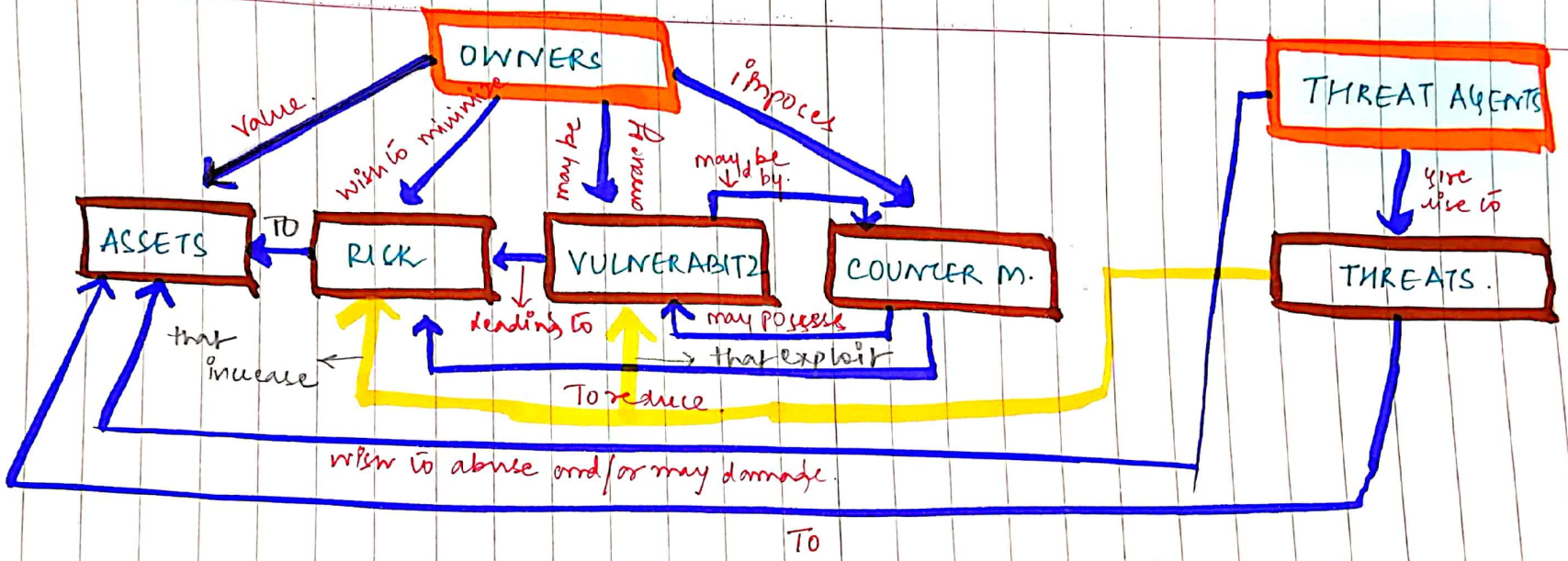
For Example :-

→ In case of a threat "spoofing the user identity" has 2 counter measures.

(1) strong authentication protocols to validate users, and

(2) Passwords should not be stored in configuration files instead some secure mechanism should be used.

Any risk still remaining after the counter measures are analyzed and implemented is called "Residual risk". (should be minimal and at acceptable level).



RISK AND RELATED TERMS.

Date :
Page No.

RISK MANAGEMENT STRATEGIES.

Tolerate / Accept the risk.

- Primary function of management is to manage risk.
- Consciously accepting the risk as a cost of doing business if appropriate as well as periodically reviewing the risk to ensure its impact remains low.

Turn back.

- where the probability or impact of the risk is very low, then management may ignore the risk.

Terminate / Eliminate the risk

- Eliminate by removing / replacing the sources of risk.

Transfer / Share the risk.

- Risk mitigation approach can be shared with trading partners & suppliers.

Treat

mitigate the risk.

- suitable controls.

Megzway

Date :
Page No.

KEY GOVERNANCE PRACTICE OF RM.

EVALUATE RISK MANAGEMENT.	DIRECT RISK MANAGEMENT	MONITOR RISK MANAGEMENT.
• continually examine and make judgement on the effect of risk on current & future use of IT in enterprise • consider appropriateness of enterprise risk apetite • Risk to enterprise value related to the use of IT are identified and managed.	• Direct establishment of RMP to provide reasonable assurance that IT RMP are appropriate to ensure that the actual IT risk does not exceed the boards risk appetite.	• monitor Key Goals & metrics of RM process • establish how deviations or problems will be identified, tracked and reported on for remediation.

Date :
Page No.

KEY MANAGEMENT PRACTISES :-

(OF RM)

1. Collect Data.
2. Analyze Risk.
3. Maintain a Risk profile.
4. Articulate Risk.
5. Define a risk management Action portfolio.
6. Respond To Risk.

METRICS OF RISK MANAGEMENT

→ % of critical business processes, IT services and IT-enabled business programme covered by risk assessment.

→ no. of significant IT related incidents that were not identified in risk assessment.

→ % of enterprise risk assessment including IT related risk

→ Frequency of updating the risk profile based on circumstances of assessment of risks.

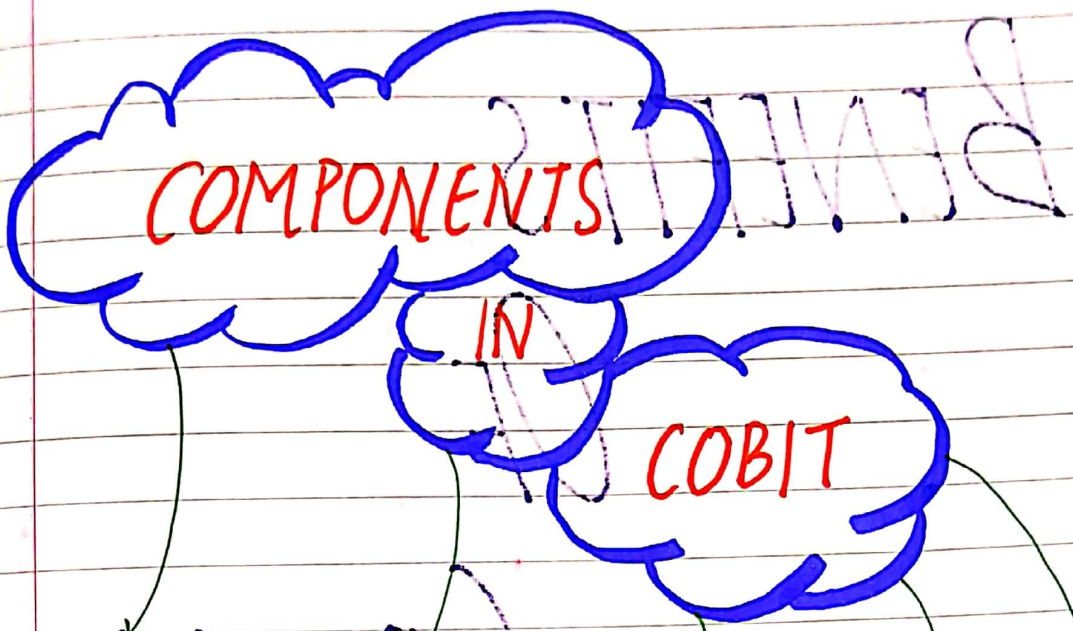
COBIT 5 :-

Control objectives for Information and Related Technology.

- A set of best practices for IT management developed by Information Systems Audit (ISACA) and IT Governance Institute in 1996.
- Set of globally accepted principles, practices, analytical tools and models that can be customised for enterprises of all sizes, industries and geographies.
- COBIT 5 also provides a basis to integrate effectively other frameworks, standards and practices such as IT Infrastructure Library (ITIL), The Open Group Architecture Framework (TOGAF) and ISO 27001.

The framework and resulting enablers should be aligned with and in harmony with the :-

Enterprise → Policies
→ Strategies
→ Governance
→ Business plans
→ Audit Approaches.
→ Risk management framework
→ Existing Governance functions, organisation, structures and processes.



FRAMEWORK.
↓
Organize IT Governance Objectives and good practices by IT domains and processes and link them to business environment.

PROCESS (PROCESS) DESCRIPTION
↓
Ref process model + common IT language for everyone + properly defined responsibility areas.

CONTROL OBJECTIVES.
↓
set of high level requirements to be considered by management for effective control for each IT process.

MANAGEMENT GUIDELINES

MATURITY MODELS.
↓
Assess maturity and capability per process and helps to address gaps.

BENEFITS OF COBIT-5

* Enables enterprise in achieving their objectives for the governance and management of enterprise IT.

** Create optimal value from IT by maintaining a balance b/w realising benefits and optimising risk levels and resource use

*** Enables IT to be governed and managed in a holistic manner.

**** manage IT related risk and ensures compliances, continuity, security and privacy.

***** Enables clear policy development and good practice for IT management

****** supports compliance with relevant laws, regulations contractual agreements & policies.

Date :
Page No.

- COBIT 5 can be tailored to meet an enterprise's specific business model, technology, environment, industry, location and corporate culture.
Because of its open design, it can be applied to meet needs related to :-
(1) Information security
(2) Risk management
(3) Governance & management of enterprise IT
(4) Assurance Activities.
(5) Regulatory and Legislative compliance
(6) Financial processing or esh reporting.

5 PRINCIPLES OF COBIT 5

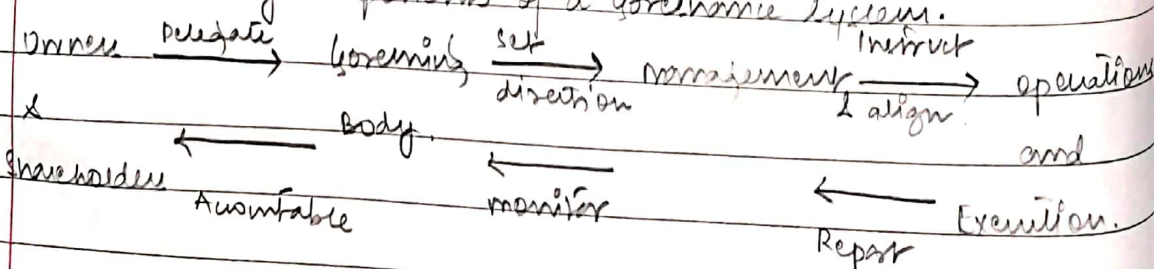
1. Meeting stakeholder needs.

→ Enterprise creates value for them by balance between realisation of benefits and optimisation of risk and use of resources.
→ Diff enterprise diff objectives, so COBIT 5 can be customised
→ Diff enterprise diff context → internal factor
→ external factor.
→ COBIT 5 goal cascade is converting or translating stakeholders needs into specific, actionable, customised enterprise goal, IT related goals and enablers.

2. Covering the Enterprise End to End.

→ It integrates governance of enterprise IT into enterprise governance.
→ Covers all functions & processes within the enterprise.
→ Considers all IT related governance and management enablers to be enterprise wide and end to end i.e. inclusive of everything everyone. (internal and external).

" Key components of a governance system. "



Date :
Page No.

3. Applying a single integrated framework.

→ As it aligns with other latest relevant standards and framework, thus COBIT 5 is an overarching governance and management framework integrator.

4. Enabling a holistic Approach.

→ Efficient and Effective governance and management of enterprise IT.

→ COBIT 5 defines a set of enablers to support the implementation of comprehensive governance and management framework.

5. separating governance from management.

→ clear distinction as these 2 disciplines have, diff type of activities, diff organisational structure, diff purposes are served.

Date :
Page No.

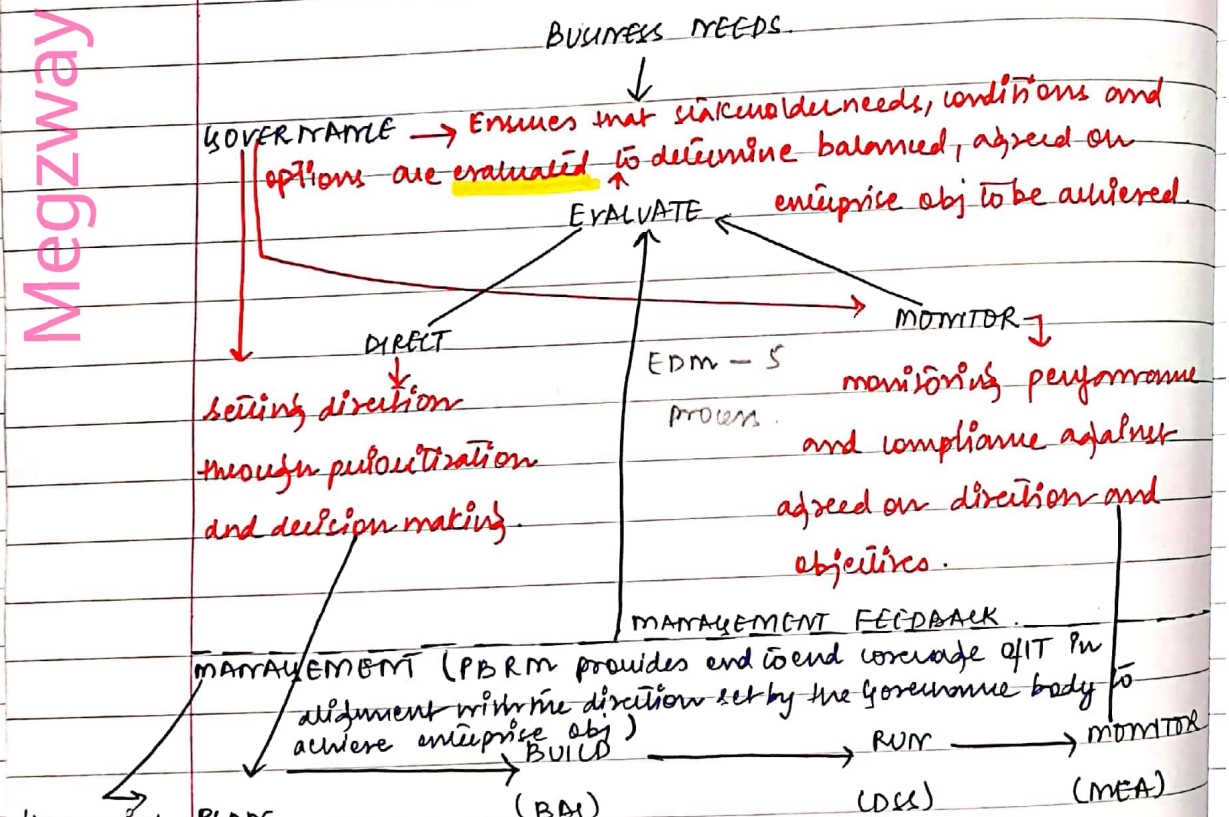
It is the successor of the COBIT 4.1 process model incorporating the both RISK IT and VAL IT framework

COBIT 5 PROCESS REFERENCE MODEL.

↳ Total 37 & 1 in process.

* COBIT 5 includes a process reference model which defines and describes in detail a no. of governance and management process of enterprise IT into two main domain governance and management.

* KEY AREAS OF GOVERNANCE AND MANAGEMENT.



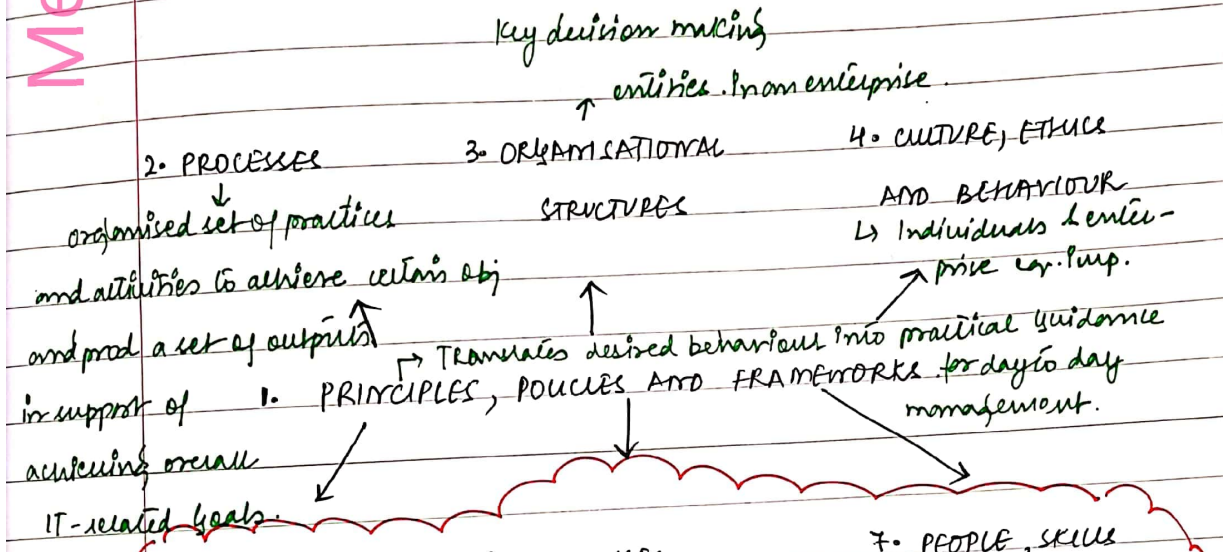
→ Responsibility of the executive management under the leadership of the CEO.

Date :
Page No.

7 ENABLERS OF COBIT 5.

→ Enablers are factors that, individually and collectively influence whether something will work; in this case governance and management over enterprise IT.

→ Enablers are driven by the goals cascade, i.e, higher-level IT related goals defining "what the diff enablers should achieve."



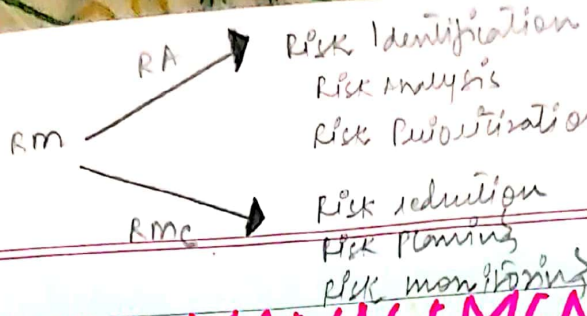
→ All info produced and used by enterprise

→ Info need for keeping the org running and well governed.

→ At operational level, info. is very often the key product of enterprise itself.

Provides the enterprise with IT processing & services.

Required for successful completion of all activities and for making correct decisions and corrective actions.



Date :
Page No.

RISK MANAGEMENT IN COBIT 5.

→ Governance domain in COBIT 5 contains 5 governance processes one of which focuses on stakeholder risk related objectives. "EDM03: Ensure risk optimisation"

This process ensures that the enterprise's risk appetite and tolerance are understood, articulated and communicated and that risk to enterprise value related to the use of IT is identified and managed.

This process provides guidance on how to ensure that IT related enterprise risk does not exceed risk appetite and risk tolerance.

→ The management domain of Align, Plan and organise, which contains a risk-related process. "APO12: Manage risk"

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

Primary purpose of this process is to integrate the management of IT related enterprise risk with overall ERM and balance the costs and benefits of managing IT related enterprise risk.

* combination of governance practices of "EDM03: APO12" ensures that RM covers the entire life cycle and covers both governance and management perspective.

* • Improvement in timely reporting of compliance issues, regular ones and remediation measures.
• Dashboard for compliance status and key issues to senior management on real time basis.

Date :
Page No.

USING COBIT 5 BEST PRACTICES FOR GRC.

→ GRC program can be implemented primarily from a compliance perspective and also be considered from business perspective. So as to optimise the investments made in implementing relevant processes, control structures and systems.

→ GRC program implementation requires the following.

- Defining clearly what GRC requirements are applicable.
- Identifying the regulatory and compliance landscape
- Reviewing the current GRC status
- Defining the most optimal approach.
- Setting out key parameters on which success will be measured.
- Using a process oriented approach
- Adapting global best practices as applicable; and
- Using uniform and structured approach which is auditable.

* Using best practices framework such as COBIT 5 can help in discharging their responsibility by ensuring that all aspects of GRC are implemented.

→ Success of GRC program can be measured by using the following goals and metrics.

- Reduction of redundant controls and related time to execute (audit, test and remediate).
- Red^{n} in control failures in all key areas.
- Red^{n} in exp relating to legal, regulatory and review areas.
- Red^{n} in process time required for audit for key business areas.

*

Date :
Page No.

COMPLIANCE IN COBIT 5

→ management domain of "monitor, Evaluate and Assess" MEA contains a compliance focused process "MEA03 - monitor, Evaluate and Assess compliance with external requirements"

↓

This process is designed to evaluate the IT processes and IT supported business processes are compliant with laws, regulations and contractual requirements. Primary purpose of this process is to ensure that the enterprise is compliant with all applicable external requirements

→ Legal and regulatory compliance is a key part of the effective governance of an enterprise

→ All enterprise activities include control activities that are designed to ensure compliance not only with the externally imposed legislative or regulatory requirements but also with enterprise governance determined principles, policies and procedures.

→ COBIT 5 framework includes the necessary guidance to support enterprise GRC objectives and supporting activities.

→ COBIT combined with COSO has been the most widely used framework for implementing IT controls as part of ERM to meet governance requirements.

Date :
Page No.

KEY MANAGEMENT PRACTICES OF IT COMPLIANCE.

COBIT 5 provides KMP for ensuring compliance with external compliances as relevant to the enterprise,
Practices are given as follow :-

Identify External compliance Requirements - continuously identify and monitor any changes to it.
Optimize Response to External Requirements - Reviewing & adjusting policies, principles, procedures with L&R Req mr
Confirm External compliance - confirm compliance of P, P, P with L&R.
Obtain Assurance of External compliance - Obtains & Report.

KEY METRICS FOR ASSESSING COMPLIANCE PROCESS.

→ Compliance with external Laws and Regulations :-
- cost of IT non compliance, including settlements & fines.
- no. of. IT related non compliance issues reported to the board or causing public comment or embarassement.
- no. of. non compliance issues relating to contractual agreement
- coverage of compliance assessments.

→ IT compliance with Internal Policies. :-
- no. of. incidents related to non compliance to policy
- % of stakeholders who understand policies.
- % of policies supported by eff standards & working practice
- frequency of policies review and update.

COBIT 5 FOR INFORMATION SYSTEM ASSURANCE

Auditors will have to understand the business processes of the enterprise and organisation structure to be effective.

↓

This understanding of the business process has to be coupled with understanding of the enterprise's policies, procedures and practices as implemented

↓

Enterprise executes its business operations through its staff

↓

staff needs to have defined job responsibilities which are provided in the organisation structure

↓

The organisation structure needs to have internal control structure

↓

IT implementation in the enterprise makes it imperative that the internal control structure is built into the IT as deployed.

↓

As IT impacts the way business operations would be performed and internal controls are implemented

↓

Hence it is critical for auditors to understand the organisation structure of the enterprise being audited as relevant to the objectives and scope of the assignment.

Date :
Page No.

↓

COBIT 5 has been engineered to meet expectations of multiple stakeholders, designed to deliver benefits to both an enterprise's internal stakeholders as well as external stakeholders.

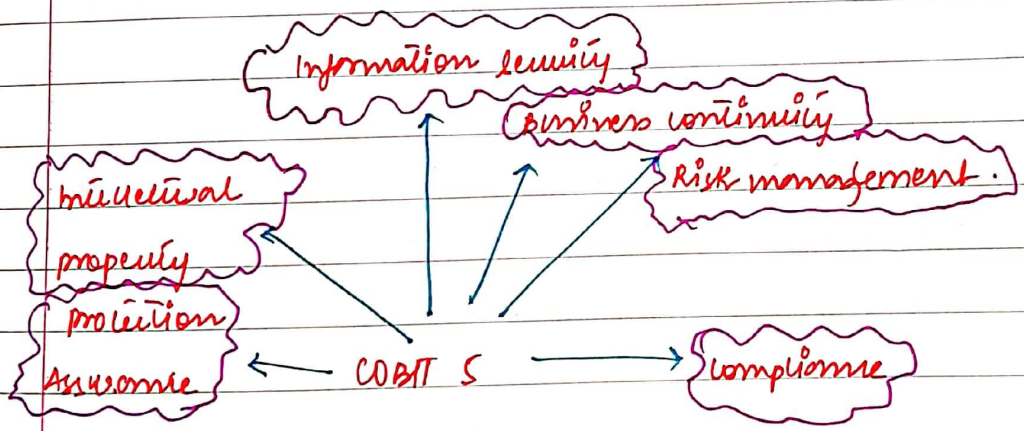
↓

It is written in an non-technical language, usable not only by IT professionals and consultants but also by senior management personnel, assurance providers.

↓

Globally from the GRC perspective, COBIT has been used with COSO by management, regulators, COBIT has been used as an umbrella framework under which other standard and approaches integrated into overall enterprise governance.

ASSURANCE NEEDS OF COBIT 5.



Evaluation Of IT Governance Structure And Practices By Internal Auditors.

→ IT governance can be evaluated by both external as well internal auditors.

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

* Internal audit activities in evaluating the IT governance structure and practices within an enterprise can evaluate several key components that lead to effective IT governance.

1. Leadership : Following aspects to be verified by the auditor

→ Evaluate the relationship between IT obj and current/ strategic needs of the organisations and ability of IT leadership to effectively communicate this relationship to IT and organisational personnel.

→ Assess → ~~Invol~~ Involvement of IT leadership in the development and on going execution of the organisations strategic needs.

→ Determine how IT will be measured in helping the org achieve these goals.

→ Review how roles and responsibilities are assigned within the IT org. and how they are executed.

6. Performance measurement/monitoring.: Following aspects needs to be verified by the auditor

→ Evaluate the framework/system in place to measure and monitor organizational outcomes where support from IT plays an imp part in internal output in IT apn and development.

2. Organizational structure : Following assessed by auditor.

→ Review how org management and IT personnel are initiating and communicating current and future needs across the organization

→ There must exist necessary roles and reporting relationships to allow IT to meet the needs of the organization.

3. Processes. : Following aspects to be checked by the auditor.

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

→ what are the process used by IT org to support IT environment and consistent delivery of expected services.

4. Risks : Following aspects needs to be reviewed by the auditor.

→ Processes used by the IT org to identify, assess and monitor/mitigate risks within the IT environment.

→ Determine the accountability that personnel have within risk management and how well these expectations are being met.

5. Controls : Following to be verified by the auditor.

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

→ Review of ownership, documentation and reporting of key validation aspects by internal audit activity.

→ control sets, should be robust enough to address identified risks based on the organization's risk appetite and tolerance level as well as compliance requirements.

IAA — Internal Audit Activity.

Date :
Page No.

SAMPLE AREAS OF GRC FOR REVIEW BY INTERNAL AUDITORS.

* Provided by IIA.

(1) → Scope : IAA must evaluate and contribute to the improvement of governance, risk management and control processes using a systematic and disciplined approach.

(2) → Governance : IAA must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives. :

→ Promoting appropriate ethics and values within the organisation.

→ Ensuring effective organizational performance, management & accountability.

→ Communicating risk and control info to appropriate areas of the org.

→ Coordinating the activities of and communicating info among the board, external and internal auditors and management.

3. → Evaluate Enterprise Ethics : IAA must evaluate the design, implementation and effectiveness of org ethics related obj, program and activities.

4. → Risk management, Interpretation, RMP. & Address Adequacy of RMP. : IAA must evaluate the effectiveness and contribute to the improvement of RMP.

Date :
Page No.

5. → **Evaluate Risk Exposure :** IAA must evaluate risk exposures relating to the org governance, operations, and IS regarding the :-

(1) Achievement of the org strategic obj
(2) Reliability & Integrity of financial and operational information
(3) Effectiveness & efficiency of op^n & programs
(4) Safeguarding of assets
(5) compliance with laws, regn, policies, procedures and contracts.

6. **Evaluate Fraud & Fraud risk :** → Potential for the occurrence of fraud, and
→ How the organisation manages fraud risk.

Date :
Page No.

SAMPLE AREAS OF REVIEW OF ASSESSING AND MANAGING RISKS.

This review:-

→ Covers the controls over the IT process of assessing and managing risks and is expected to provide assurance to the management that the enterprise has identified all the risks relevant to the enterprise/business as relevant to IT implementation.

→ Provide assurance that it has app risk management strategy to mitigate these risks.

→ Specific areas evaluated are:-

- Risk management ownership and accountability
- Different kinds of IT risks.
- Defined and communicated risk tolerance profile
- Root cause analyses and risk mitigation measures
- Quantitative and/or qualitative risk measurement.
- Risk assessment methodology
- Risk action plans and Timely reassessment.

Date :
Page No.

EVALUATING AND ASSESSING THE SYSTEM OF INTERNAL CONTROLS.

COBIT 5 has a specific process : MEA02 – monitor Evaluate and Assess the system of IC.

which provides guidance on evaluating and assessing internal controls implemented in an enterprise.

Objective of such review is to :

- continuously monitor and evaluate the CE
- Enable management to identify management deficiencies and inefficiencies and to initiate improvement actions
- Plan, organise and maintain standards for IC assessment and assurance activities.

Key management practices for assessing and evaluating the system of IC in an enterprise are given as follows :-

→ monitor IC.
→ Review Business process control effectiveness.
→ perform control self assessment.
→ Identify and report control deficiencies.
→ Assure that assurance providers are independent & qualified.
→ Plan, scope & evaluate assurance initiatives
→ Identify and report control deficiencies.