chapter-1

Governance & Management of Information systems

by Hari Krishna Gatti

Chapter-1

Governance and Management of IS

1- **IT Governance**:- It refers to the system in which directors evaluate, direct & Monitor IT Management to ensure effectiveness, accountability and Compliance of IT.

Benefits of IT Governance

1. Increased Value delivery through Enterprise IT
2. Increased User Satisfaction with IT Services
3. Improved agility in supporting business needs
4. Compliance with relavant laws & Regulations
5. Reduce Costs.
6. Optimal utilization of IT Resources.
7. IT become enabler for Change rathar than inhibitor
8. Mitigate IT related Risks.

2. **GEIT (Governance of Enterprise IT** is a subset of Corp Gov.
Primary objectives of GEIT is to analyse & articulate the requirements for governance of Enterprise IT.

Benefits of GEIT

1. Provides consistent approach aligned with enterprise governance
2. Ensure IT related decisions are inline with Enterprise Strategies
3. Ensure that IT related processes are overseen effectively
4. Comfirm compliance with legal & regulatory frame
5. Ensure Governance requirements for Board mem are met.

Key Governance practices of IT

1. Evaluate Governance System.
2. Direct the Goverance System
3. Monitor the Goverance System.

3. **Enterprise Risk Management**:-
Sarbanes Oxley Act (SOX) uses COSO - Committe of Sponcering Organisation, as one of the important guidelines for implementing Risk management and internal Controlls.

4. **Internal Controls as per COSO - CRAIM**
1. Control Environment - develop & maintain a Control Environment
2. Risk Assessment - CE must include an ass of risk associated with E
3. Control Activities must be developed to manage, reduce, mitigate the ris
4. Information & Communication
5. Monitoring: - Int controlls must be continously monitered.

5. **Clause 49 of SEBI** are in similar line with SOX regulations

6. **IT Steering Committee**:- A high level Committe to provide appropriate direction to IT deployment & IS to ensure that IT deployment is in tune with enterprise objectives.
IT steering Committe Consits of heads from all departments and are responsible for taking decisions related to their departm

Key Functions of Steering Committee

1. Ensure long & Short term plans of IT are inture with Ent.
2. Approve & Review a major IT deployment projects.
3. Approve & Review key projects & measing results (ROI)
4. Review the status of all IT Plans
5. Review standards, policies and procedures.
6. Facilitate implementation of IT Security.
7. Facilites & Resolve conflicts in deployment of IT.
8. Report to BOD on IT activities on regular basis.

Risk Management:-

* Risk is the possibility of Something may happen adverse.
* Risk Management involves identifing, measuring and minimising untain events effecting the resources.
* Auditors are required to check wther proper and adequate controls are there to mitigate Risk.

Source of Risk

a. Commercial & legal relations
b Economic Consequences
c. Policital Circumstance
d Natural Events
d. Human behaviour
e. Technology issues.

Risk Management Strategies: "IIIII"

1. Tolerate or Accept Risk: Accepting Risk as a part of busines.
2. Terminate/Eliminate Risk: when risk is related to particular, trader, technology or Vendor, Risk can be elimated by replace.
3. Transfer/share Risk: Risk can be mitigate by sharing with Trading partners and suppliers. Ex: Outsourcing Infra Mgmt. Risk can also be transfer to insurance ltd.
4. Treat the risk: After using methods to eliminate risk, use suitable controls to prevent from manifest of Risk.
5. Turn back: If risk is very low ignore it.

Key Governance Practices of Risk Managements.

Evaluate RM - Continual examining and make judgements on Risk
Direct RM - Direct the enterprise on RM pactices
Monitor RM - Moniter key goals and metrics of RM

Key Mgmt Practices of Risk Management: - CAAARR

1. Collection of Data
2. Analyse Risk
3. Maintain Risk profile
4. Articulate risk to stakeholders
5. Define risk Action Porpolal
6. Respond to Risk.

Metics of Risk Management.

1. % of Critical business Processes
2. No of Significant IT related incidents
3. % of ent risk assmts
4. Frequency of updation

8. Cobit 5 (Controlled OBjectives for Information & Techn
is a set of best practices for IT mgmt developed by ISA
Cobit 5 is a business framework for Governance and Mng
of Enterprise Info technology. It incorporates latest thinking
in Enterprize Governance and Management tegniques &
provides globally accepted Principles, Practices, tools and
models to help increase trust in value from IS.

Benifits of Cobit 5 - ROC - ~~LFFS~~ - OC HR PAL

1. Enables enterprise in acheiving their objectives for Governanee & Mgnt of Enterprise IT.
2. Helps enterprises to create optimal value from IT by maintaining a balance between Realising benifits & Risk leve and resource use
3. Enable IT to be governed and managed in a holistic manne taking end-to-end IT functions of Responsibility, Considering IT related interest of Internal & External Stake
4. Helps Enterprises to managed IT related risk and Ensure Compliance Continuity, Security & Privacy.
5. Enables clear policy development & good practice for IT mgnt including user satisfaction.
6. Key Advantage of Cobit 5 is, it is useful for enterprise of all levels & Sizes and types.
7. Support Compliance with Laws & Regulations, & Policies

Components in COBIT 5 CM caludating FMP

* Frame Work - Organise IT Governance by IT domains & proces and link them to business Requirements
* Process Description:- A reference processess model and common language for everyone in an Organisation.
* Control Objectives:- Provide a Complete set of high level requirmn to be considered by mgnt for effective control o each IT Practice.
* Manage Guidelines: Help assign responsibilities, agree on objectiv measure performance.

Maturity Models: Assess maturity & Capability, per process.

Five principles of COBIT 5 - MESH-S

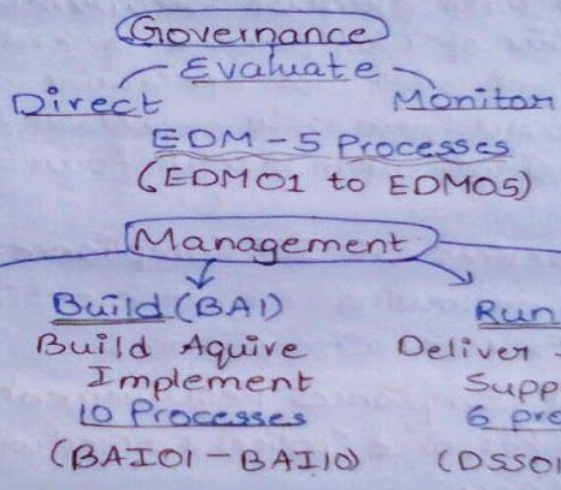
Cobit 5 Simplify Goverance with just 5 principles.

1. Meeting Stake holders Needs: Cobit-5 Enables all required processes to support, business value creation.
   Cobit 5 "Goal Cascade" mechanism helps to translate stakeholders needs & into specific, actionable, & Customi enterprise goals, IT realted goals and enabler goals.
2. Covering Enterprise End to End: Cobit 5 covers all the functions with in the Enterprise It doesn't focus only IT function, but treats Information & Related technologie

as assets that needs to be treat like any other assets by everyone in Enterprise.

- **Single Integrated Framework:** There are many IT related best practices providing subsets of IT activities. COBIT 5 is a single integrated framework which includes all other relavant standards & frameworks, thus allowing enterprise to use Cobit 5 as an overarching Gov & mgnt frmwk ingrtor.
- **Enabling a Holistic Approach:** Cobit 5 defines a set of Enablers to support the implementation of Comprehensive Governance & mgnt of Enterprise IT. thus providing a Holistic approach.
- **Separating Governance from Management:** COBIT 5 makes clear distinction between Governance & Management. Both are different disciples require different structure & Serve different purposes.

COBIT 5 Process Reference Model:- 2 models.



Seven Enablers of Cobit 5 :

Enablers are driven by Goals Cascade. Cobit 5 defines 7.

1. **Principles, Policies & Framework** are vehicles to translate Desired behavior into practical guidance.
2. **Processess.** these are organised set of principles and practices & activities to acheive certain objectives in support of overall IT.
3. **Organisational Structures:-** are the key decision making Entities
4. **Culture, Ethics & Behaviour** of Individual & Enterprise is an important factor for Success of Gov & Mgnt activities
5. **Information:** is persuasive & include all info used by Enterprise
6. **Services, Infrastures, & Applications:** are the technology & application that provide enterprise to IT processing & Services
7. **People, Skills & Competence:** are linked to people and are required for Successful Completion of all activities.

Risk management in COBIT-5.

EDM03 - Ensure Risk Optimisation (Governance domain)
APO12 - Manage Risk (Management domain)

EDM03:- This process ensures that enterprise risk appetite is understood, articulated and risk to enterprise value related to IT is identified & Managed. This provide that how to ensure that IT related Enterprise Risk is does not exceed Risk appetite and Risk tolerance level.

APO12:- This process requires continous identifing, assesing and reducing IT related risk with in the levels of tolerance level set by Executive management.

Thus both EDM03 & APO12 togather ensure that Risk mgmt covers entire life of the Cycle & covers both Governance & Management perspective.

Compliance in Cobit5.

MEA03 - Compliance with External Requirements.

The primary objective of this process is ensure that the Enterprise is Compliant with all applicable External Regulation. COBIT along with COSO provides excellent framework for implementing IT Control with special focus on Compliance activities

Key Management Practices of IT Compliance:

COBIT5 provides following mgmt practices for ensuring Compliance with External Compliances.

(a) Identify External Compliances Requirement
(b) Optimise (adjust) Response (polices & procedures) to E. Requirement
(c) Confirm Compliance
(d) Obtain assurance of External Compliance.

Key metrics for Assuring Compliance.

(a) Compliance with External laws
   i. Cost of Non Compliance
   ii. No of IT related noncompliance causing embarrismt
   iii No of Non Compliance issed with IT Service providers
   iv. Coverage of Compliance assesments
(b) Compliance with Internal policies.
   i. No of instances of Non Compliance.
   ii. % of policies Supported by E. Management
   iii % of stakeholders who understand policies.
   iv. % of frequency of review & updation

COBIT 5 for GRC (Governance, Risk, Compliance).

Successful implementation of GRC, can be measured in terms of assurance provided to Senior mgmt. However specific Success of GRC program can be measured by using following Goal & Metrics.

a. Reduction of Redundant Controll
b. Reduction of Control failure in all area
c. Reduction of Expenditure relating to legal Expense.
d. Reduction of overall audit time.
e. Improvement of process
f. Improvement in timely reporting
g. Dashboard to overall compliance status.

Evaluating IT Governance Structure & Practice by IA.

As per IIA following aspects should be reviewed by I. Auditor
a. Leadership b. O. structure. c. Risk d. Processes e. Performance

Sample Areas of GRC to be reviewed by Internal Auditor.

a. Scope
b. Governance
c. ~~External~~ Evaluate Ethics in Enterprise
d. Risk mgmt
e. Evaluate Risk Exposure
f. Risk managmt process
g. Evaluate Fraud
h. Address adequacy of Management process.

Management practices for Aligning IT strategy with Ent Stty.

1. Understand Enterprise Direction.
2. Assess the Current Environment Capabilities
3. Define Target IT Capabilities
4. Conduct a Gap Analysis.
5. Define strategic plan & roadmap
6. Communicate the IT strategy & direction