- CA Sukriti Jain sukriti9225@gmail.com

CHAPTER 1 – Concepts of Governance & Management of IS

Governance- to steer

- refers to mechanisms
- for evaluating options,
- setting direction &
- monitoring compliance & performance,
- to satisfy specific entrp obj.

Benefits of Governance [RDADIES]

i. Improving customer Relationships & integrating into holistic IT governance framework; user satisfaction
ii. Achieving entrp Obj
iii. Aligned decision making for IT (Alignment of IT with Biz)
iv. Desired biz process
v. Encourage Desirable Behavior in the use of IT
vi. Providing Stability to organizational Structure

Based on above it can be seen that IT is an integral part of governance.

Enterprise Governance

- The set of responsibility & practices exercised by BOD & mgmt
- with goal of
- providing strategic direction,
- ensuring that obj are achieved,
- risks are managed &
- org resources are used responsibly.

* IT is key enabler of corp biz strategy. alignment b/w IT & biz obj is a CSF to achieve biz obj

* corp gov - it is resp of top (M) to ensure every activity is controlled & directed to achieve obj of SH.

Enterprise Governance Framework / Governance Dimensions-

Corporate Governance (Conformance)	Business Governance (Performance)
• System by which a co. is directed & controlled to achieve the obj of Increasing shareholder value by enhancing economic performance.	• Biz oriented &
• covers roles of chdirman/CEO, BOD (M), control assurance & risk Mgmt.	• takes Forward Looking view &
• BOD are accountable to SH.	• Pro-active approach
• provides historic view	• Focus on Strategy & Value Creation
• focuses on compliance with regulatory requirement	• Develop Best Practices, Tools; eg- Balance scorecard Techniques, to achieve biz obj
• Oversight Mechanisms - Audit	• Understand risk apetite & key performance drivers
• to ensure that good corp gov process are effective - sustainable & eco devlp.	• Not governed by any standards & assurance. Specific to entrp goals & varies accordingly
• SOX & Clause 49 require Conformance.	• No dedicated oversight mechanism.
	• Full responsibility of board (advisable to establish oversight committee)

These 2 dimensions must be balanced to meet stakeholders reqm & to ensure long term success.

IT Governance-

IT Gov is a system in which directors of entity, evaluate, director, monitor – IT activities to ensure effectiveness, accountability & compliance of IT.

system by which IT activities in co. are directed & controlled to achieve biz obj with ultimate obj of meeting stakeholder needs. overall obj of IT gov is similar to corp gov but with focus on IT. IT Gov is a sub-set of CG & EG.

GEIT

GEIT is sub-set of Corp Gov & facilitates implementation of IS controls in enterp. in all key areas

Objective-to analyze requirement of gov of IT in entrp & to put, maintain effective structures, principles, processes, practices to achieve the enterprise goals. (with clarity of Resp & Auth)

It is macro / broader than IT gov

Benefits of IT Gov - increased (VALUER CO)

1) ↑ Increased Value delivered by IT — value ↑
2) ↑ Improved Agility in supporting biz needs — Agility
3) ↑ compliance with Laws; — Compliance ↑
4) ↑ User satisfaction with IT — user ☺ ↑
5) IT = Enabler for change
6) ↑ Optimal utilization of IT Resources. — use opt Resource
7) ↓ Better Cost performance of IT; — cost ↓
8) Improved Transparency of IT's contribution to biz
9) ↓ Improved Mgmt & Mitigation of IT-related biz risk; — Risk ↓

Benefit of GEIT – ensure - [P-CARD]

IT-related Processes managed effectively
Compliance with legal & regl req
Approach aligned with Entrp Gov Approach.
Gov Reqm are met.
IT-related Decisions made in line with entrp obj.

Key Gov Practices OF IT Gov-

Who makes directing, controlling & executing decisions
What info req, How decisions made, mechanism, exceptions handling, monitor & improve Gov Results.

Key practices which determine status of IT gov in entrp ?

Key Gov Practices of GEIT [EDM]

Evaluate gov system – current & future IT gov.
Direct " " – (M) support & guide structure & processes
Monitor " " – effectiveness & performance of GEIT.

COSO is the Std of I.C. Cobit is the Std of IT Gov. ISO is for info security

Best Practices of Corp Gov – (AMIIIR) Best Practices

A 1. Clear Assignment of resp & decision-making authority,
I 2. Establish Mechanism for interaction & cooperation among BOD, Top (M) & auditors;
I 3. Implement strong internal control systems
M 4. Financial & Managerial incentives to senior management, & employees
I 5. Appropriate information flows internally & to public
R 6. Special monitoring of Risk exposures where conflicts of interest are more

ERM – holistic & comprehensive approach

- Integrated Framework published by COSO.
- It is a process, effected by an entity's BOD, mgmt & other personnel, applied in strategy setting across the enterprise, - overall Risk(M) strategys @ all level of entrp
- designed to identify potential events that affect the entity,
- & manage risk to be within its risk appetite,
- to provide reasonable assurance to achieve entrp obj.
- IT security & controls are a sub- set of the overall ERM strategy.

"INTERNAL CONTROL over financial reporting" – To make B/S T&F & as per GAAP

is a 'process designed by company's principal executive & financial officers, & effected by the company's BOD, management & other personnel, to provide reasonable assurance regarding reliability of financial reporting & preparation of financial statements as per GAAP & policies & procedures that ensure – recording of all txn, proper authorizations, accurate records of assets, prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that have a material effect on the financial statements."

Resp of IC as per SOX -

- SOX holds CFO & CEO personally & criminally liable for effectiveness of IC,
- IC provide only a reasonable assurance, not an absolute assurance.
- fin st. shud comply with AS.
- must be a system of checks & balances for proper reporting of txn.

IC as per COSO: (CRIME) (FTP)

IC has 5 interrelated components:

1. Control Environment – Tone at Board
2. Risk Assessment – Id. risk
3. Control Activities – Reduce risk
4. Information & Communication – ev. should be aware
5. Monitoring – effectiveness of IC & modifications if needed

Clause 49

of the listing agreements issued by SEBI in India is in line with SOX & mandates the implementation of ERM & IC & holds the senior mgmt legally responsible for implementation of IC. Also, External auditor is required to provide certification on these aspects.

ROLE OF IT IN ENTERPRISES

- Today Biz is dependent on IT. IT fails -> Biz fails
- Today IT not merely for Data processing, but for Strategic & competitive advantage too.
- Not only Automated Biz process & also Transform way of doing biz process.
- IT not only info proceeding tool, but also better & innovative services.
- Hence, Mgmt shud devlop a IT strategy, aligned with biz strategy, to ensure value creation & benefit realization from IT investment. & also do IT gov.

Business & IT Strategy ("To develop IT strategy org" shud know biz strategy & vice versa)

Biz ↓↑ IT

- Management Strategy, determines the overall path & methodology of rendering service
- Integration of IT strategy with biz strategy
- Auditors should be involved in providing assurance related to info systems & internal control system.
- strategies & tactics of IT department to ensure effective day to day IT operations
- Metrics & goals established to measure IT perform on a tactical basis
- Internal audit can measure progress of IT strategy & its alignment with biz obj.

IT Steering Committee

form by Top (M) to monitor IT dept

Sr. Mgmt may appoint a high-level committee to provide appropriate direction for IT development & implementation & to ensure that IT is in line with biz obj. Led by members of BOD & consist of functional heads of deptt (incl (It) & Audit) planning related to IT info sys is undertaken by SC & Head of Dept + Auditor + IT experts

Key functions of IT Steering Committee – ✱✱

1. review & approve IT deployment projects
2. review & approve standards, policies & procedures
3. review status of IS plans & budgets & overall IT performance
4. establish size & scope of IT function & sets priorities
5. ensure that long & short-range IT plans are in tune with Biz obj
6. To make decisions on IT deployment & implementation
7. resolve conflicts in deployment of IT
8. implementation of IT security
9. Monitor key projects by measuring result of IT projects in terms of ROI
10. To report to BOD on IT activities on a regular basis.

IT Strategy Planning- *Planning* = deciding in advance = what is to be done', who is going to do' & when it is going to be done'. It provides direction to deployment of info systems. IT plans shud be communicated to biz process owners & other users & establish a process to get feed back from them, on quality & usefulness of plans. Sr. mgmt is resp for developing & implementing long & short-range plans to achieve entrp mission & goals. IT Plans should ensure that use of IT is aligned with the mission & biz strategies of the entrp. ensure that IT strategic plans are aligned with biz strategic plans as IT is ultimately used for achieving biz obj. Strategic planning could be done by the top management or steering committee. Strategic planning puts organization objectives into time-bound plans & action; helps to ensure an effective & efficient enterprise; & also address & help determine priorities to meet business needs.

There are 3 levels of managerial activity in an enterprise: (3 levels of managerial planning)

- Strategic Planning – top @ determine overall org^n obj & how to achieve them
- Management Control – Managers ensure that resources are obtained & used effectively & efficiently
- Operational Control – ensure that specific tasks are carried out effectively & efficiently

IT Strategic Planning Process

- establish Policy to develop & maintain, IT long & short-range plans
- modify IT long-range plan to accommodate changes to entrp long-range plan & changes in IT conditions. Δ plan as per Envt
- regularly translate IT long- range plans into IT short-range plans. long → short
- allocate IT resources, on a basis consistent with IT long-range plan. Resource allocate करने के लिये need है to execute plan
- Periodically reassess short-range plans & amended in response to changing business & IT conditions.
- Perform feasibility studies to ensure that execution of short-range plans is adequate.

Objective of IT Strategy

To provide holistic view of current IT env,
Set future direction & Take initiatives reqd to migrate to desired future environment.
Align strategic IT plans with biz obj, by communicating obj & associated accountabilities, so they are understood by all.

Classification of Strategic Planning - Info Systems planning undertaken by top M to meet long-term objectives of entrp. IT Strategy planning can be classified into following **categories**:

(ESRA)

- Enterprise Strategic Plan,
- IS Strategic Plan,
- IS Requirements Plan, &
- IS Applications & Facilities Plan.

Enterprise Strategic Plan- (Biz obj)

the primary plan **prepared by top mgmt**, that guides long run development of entrp.
It provides overall charter,
– statement of **mission**,
– **specification of strategic objectives**,
– assessment of env & org factors
– statement of **strategies for achieving the objectives**,
– Constraints
– a listing of **priorities**.
In an IT environment, it is important to **ensure that the IT plan is aligned with the enterprise plan**.

IS Strategic Plan: (IT obj)

focus on optimum balance of IT opportunities & IT business reqmt. entrp reqd to take stragic planning process at regular intervals. **Some ENABLERS of IS Strategy plan are:**

1. Enterprise biz strategy,
2. Define how IT supports Biz obj,
3. technological solutions & current infrastructure,
4. Monitor technology markets,
5. Timely feasibility studies & reality checks,
6. Existing systems assessments,
7. Enterprise position on risk,
8. Need of senior management support & review.

Information Systems Requirements Plan: (क्या चाहिए)

It defines information system architecture needs of the entrp. This requires creation & continuous maintenance of a biz info model ensuring that systems are defined to optimize use of info. IS Requirements Plan drawn up, based on info architecture reqm, to meet the info reqm of entrp. IS architectur will determine the info need & flow in an entrp.

Some key ENABLERS of the info architecture are-

1. Enterprise architectural **standards**.
2. Data syntax **rules**,
3. **info model** representing biz
4. Automated data repository & **dictionary**,
5. **Data ownership** & criticality/security **classification**,

Information Systems Applications & Facilities Plan:

On the basis of IS architecture, Mgmt can develop IS appl & facility plan. This plan includes:

- **Application systems** to be developed & associated time schedule,
- **Hardware & Software** acquisition/development schedule,
- **Facilities reqd**
- Organization **changes** reqd

(physical implementation to plans)

How to make IT in Tune with Biz ? (May'15)

① **Key Management Practices** for Aligning IT Strategy with Enterprise Strategy

1. Understand enterprise direction – consider current env & future obj. – what biz wants.
2. Assess current environment, capabilities & performance – assess current IT performance, & issues & problems faced – eg - IT is Too Slow
3. Define target IT capabilities – क्या चाहते हैं – fast IT
4. Conduct Gap analysis – identify gap b/w ② & ③
5. Define strategic plan & road map – Develop strategies to close gap & monitor achievements. define how IT related goals will contribute to entrp strategic goals
6. Communicate IT strategy & direction – सबको Aware करो उसके बारे में | Create awareness & understanding of Biz & IT obj & directions

Business Value from Use of IT

It is achieved by ensuring optimum value from biz processes, IT services & IT assets resulting from IT-enabled investments at an acceptable cost. It ensure that entrp is able to secure optimal value from IT, cost-efficient delivery of services, & a picture of cost-benefits.

② EDM

KEY MANAGEMENT PRACTICES, which need to be implemented for evaluating 'Whether business value is derived from IT'-

- Evaluate Value Optimization. – whether IT invt portfolio, deliver value @ reasonable cost & achieve entrp obj
- Direct Value Optimization. – Direct value ⓐ principles & practices.
- Monitor Value Optimization – Monitor the extent to which IT is generating expected value & benefits to biz. identify issues & take corrective actions

① **KEY METRICS, which can be used to measure the benefits realized** from IT enabled investments & services portfolio, are: (RTP)

- % of IT investments where benefit realization monitored throughout economic life cycle; (चाहिए)
- % of IT services where expected benefits realized; (मिला)
- % of IT investments where claimed benefits met or exceeded; (उम्मीद से ज्यादा) (Same Q Pg 7)
- % of investment business cases with clearly defined & approved expected IT related costs & benefits;
- % of IT services with clearly defined & approved operational costs & expected benefits
- Satisfaction survey of key stakeholders regarding the transparency, understanding & accuracy of IT financial information (achha)

Biz से IT के cost benefit
IT से Biz के cost benefit
Satisfaction.

corpgov ERM ITRM

RISK MANAGEMENT

Risk is the possibility of something adverse happening, resulting in potential loss/exposure.
Risk mgmt is the process of ***identifying*** risk, ***assessing*** risk, taking steps to ***reduce*** risk to an acceptable level & maintaining that level of risk.
Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks.

step1

Sources of Risks (8)

- o Commercial and Legal Relationships
- o Economic Circumstances
- o Human Behavior
- o Natural Events
- o Political Circumstances
- o Technology & Technical Issues
- o Management Activities & Controls,
- o Individual Activities.

Characteristics of Risk:

- *Loss potential* – When threat exploit weakness
- probability/*Uncertainty of loss* of such loss;
- *Likelihood of threat* agent causing attack

Risk Related Terms (Risk Assessment Approach)

step 2

ASSET: 3 Characteristics –
o **Value** to the org
o not **replaceable** without **cost/time/resources**.
o Part of **corporate identity**
o **Data Classification** – proprietary, Highly confidential, top secret

VULNERABILITY: **weakness in system safeguards, that expose system to threats.** Eg- no lock on door, weak pwd. Weakness, **that could be exploited by a threat**. Vulnerabilities potentially "allow" a threat to harm or exploit the system. Eg - poor access control method allow dishonest employee (threat) to exploit system------Leaving door unlocked makes house vulnerable to unwanted visitors----Short pwd make info system vulnerable to pwd cracking.

Missing safeguards often determine level of vulnerability. Determining vulnerabilities involves a security evaluation of system including inspection of safeguards, testing & penetration analysis. Vulnerabilities can originate from flaws in software's design, defects in its implementation or problems in its operation. 'vulnerability' means opening doors for attackers. **Vulnerability must have at least one of the following conditions -**

- 'Allows an attacker to **execute commands as another user'** or
- ' " " " to unauthorized **access data'** or
- ' " " " to **pose as another entity'** or Masquerading
- ' " " " to conduct a **DOS.**

THREAT: **event with capability to harm the system,** through its unauthorized access, destruction, modification or DOS. It is an action which will compromise system's quality & ability to inflict harm to the org. it has capability to attack on a system with intent to harm. A threat cannot exist without a target asset. It is prevented by applying some sort of protection to assets. ~~Eg – unauth access, destruction, modification or denial of service, etc~~

potential /

EXPOSURE: **extent of losses, when risk materializes**. both immediate & long run impact. Eg- ICICI hacking – loss of reputation, privacy, confidentiality, data loss, etc

[No weakness = No Threat = No Exposure]

LIKELIHOOD : **estimation of the probability, that threat will succeed in achieving an undesirable event.** The presence & strength of threats, as well as the effectiveness of safeguard must be considered while assessing the likelihood of the threat occurring.

(Risk = Threat + weakness)

to defeat security

ATTACK : **attempt to gain unauthorized access into the system**. any action which will *compromise CIA of info system*. It is a malicious intentional act, usually external fault, with the intent of exploiting vulnerability in the targeted software or system. It is an act of **trying to defeat Information Systems (IS) safeguards**. The type of attack & its degree of success determines the consequence of the attack.

RISK : potential **damage to asset caused** if **(weakness + threat).** [Risk = standard safeguards- actual safeguards] potential harm caused, if a particular threat exploits a particular vulnerability to cause damage to an asset.

RISK ANALYSIS: **process to identify security risks & their impact on org.**
Risk Assessment incl - Identify threats & weakness
- Potential Impact on CIA, when threat exploits vulnerability : Priority of threats
- analyse Security controls

Information systems generate many Risks. These risks lead to a gap between **need to protect systems & degree of protection applied**. The **gap is caused by:**

(DECEITD) (DELET IT)

- D • **Devolution** of mgmt & **control**
- E • Attractiveness of conducting **unconventional (E-) attacks** against org
- T • Unevenness of **technological Changes**;
- L • **External factors** like legislative, legal & regl reqm or technological developments.
- I • **Interconnectivity** of systems;
- T • Widespread use of **Technology**;
- E • Elimination of **Distance, time & space** as constraints;

(Risk ↓)

COUNTER MEASURE : Any action/ device/ technique which reduces vulnerability of system. Eg- antivirus is CM for virus. For eg, well known threat 'spoofing the user identity', has two countermeasures:

- **Strong authentication protocols** to validate users; &
- **Pwd not to be stored in configuration files** instead some secure mechanism should be used.

RESIDUAL RISK: Risk still remaining after implementation of counter measures. but cant be eliminated. Residual risk must be kept at a minimal, acceptable level. risk can be minimized, acceptable level. **management of risk** should consider these **2 areas**: acceptance of residual risk & selection **of safeguards** Risk M Approach regularly communicates status of Residual Risk to stake holders to manage IT Risk profile.

Risk ko counter karne keliye → Controls lagao (Not alwz Appropriate) / Strategies to Manage Risk

Risk management strategies (TS) (Step 3)

- **Tolerate**/accept the risk → Minor Risks, bcz low probability, Impact. Dont think about control till it is within acceptable limits. & Review it periodically to ensure its impact remains low
- **Terminate**/eliminate the risk → Replace the Technology/ vendor, which is causing risk. eg- dont use wifi use LAN.
- **Transfer**/share the risk → share risk with Trading partners, suppliers, eg - Insurance, outsource Infrastructure.
- **Treat**/mitigate the risk → implement appropriate controls to prevent risk or minimize impacts eg- Anti for virus.
- **Turn back** → probability/impact of Risk is very low Just ignore eg- Earthquake in Gwl

Step 4

(3)

Key Governance Practices of Risk Management

1. *Evaluate Risk Management* – whether IT Risk is within Risk apetite & effect of Risk on current & future IT.
2. *Direct Risk Management* – If NO → then establish Risk (M) by Top (M)
3. *Monitor Risk Management* – Monitor goals & metrics of Risk (M) process & identify deviations & report for remedy.

Step 5

Key Mangement Practices for implementing Risk Management:

[CAP AAR]

(3)

1. *Collect Data* – Identify IT Related Risk
2. *Analyze Risk* – out of which, identify IT related Risk having Biz impact
3. *Maintain a Risk Profile* – List of risks, their attributes & impact in to decide priority
4. *Articulate Risk* – Communicate current IT Related exposures to Stakeholders.
5. *Define a Risk Management Action Portfolio* – plan of action / controls to Manage risk
6. *Respond to Risk* – Actual implementation of controls. Take effective measures to limit the magnitude of loss from IT related events.

Step 6

(2) ***Metrics to monitor IT Risk Management:*** to monitor the ITRM.

1. Percentage of **critical business processes** & IT services covered by risk assessment
2. No. of **IT related incidents** that were **not identified** in risk Assessment
3. Percentage of enterprise risk assessments including **IT related risks** & (ITRM / ERM)
4. **Frequency** of **updating risk profile** based on status of risk assessment.

(same Q pg. 4)

Risk Management by COBIT 5?

organisation can manage risk without COBIT also, but it won't be effective. COBIT5 provides detailed guidelines, frameworks, standards & practices, which is developed by experts across the globe, to treat IT related risk. That is why organisation follow COBIT 5 to reduce level of risk.

Governance Domain of COBIT focus on stakeholder risk related objectives – **EDM 03 -ensure risk optimization.** Ensure that IT risk does not exceed risk appetite & risk tolerance. Direct how risk faced by org will be treated.

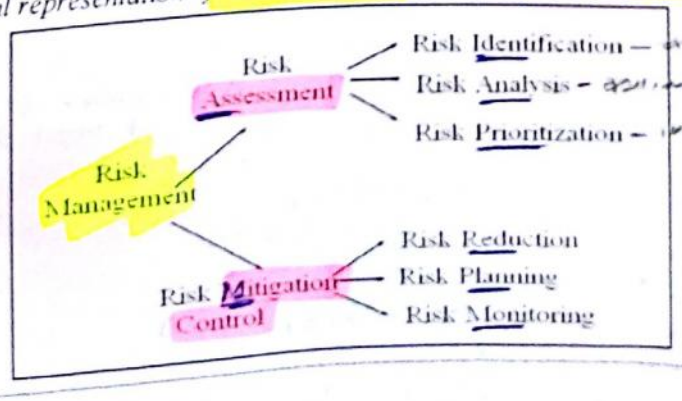
Management Domain of COBIT – **APO 12 -Manage Risk** – continuously identify, assess & reduce IT-related risk within tolerance level. Integrate Management of IT related Entrprise risk with overall ERM & baance the cost & benefits of manging IT related enterprise risk.

Combination of both domains ensure that Risk management covers entire life cycle & both Gov & (M) perspective of Risk.

Cobit suggests Accountabilities, Responsibilities & risk related Roles at each level of Mgmt.

(AQ)

A pictorial representation of various activities relating to risk management is given below-



IS के implementation के लाभ में check करो कि वो सही में चल रहा है
& CA से assurance देने के लिए क्या tools use करेगा?

Information Systems Assurance

Examples of diff Assurance Needs of COBIT 5 performed by using COBIT 5 — Assurance Needs, which can be:
- Info security
- Risk (M)
- Assurance
- Compliance
- Biz continuity
- Intellectual property protection

Auditor para

Using COBIT 5 for IS Assurance

- Auditor to understand biz process & org structure & biz policy & procedures, to be effective
- Assign proper job responsibilities to IT staff. Proper Internal control structure
- Cobit Meet expectations of multiple stakeholders
- Cobit deliver benefit to both internal & external stakeholders - (E), employee BOD ; customer, Sh., supplier, auditor
- Written in a non-technical language- usable by all
- From GRC perspective, Cobit widely used with COSO, for implementing Gov & Mgmt practices from end to end perspective
- Umbrella framework integrating other standards

(POLICE RCM) Auditor

Evaluating IT Governance Structure & practices by Internal Auditors:

1. *Leadership* – top(E) participation, roles & respo assign, relationships b/w IT & obj & biz needs.
2. *Organizational Structure* – evt stnd know their roles & respo. & how they interact
3. *Processes* – process to mitigate risks are effective
4. *Risks* – how org" identifies, monitor & mitigate risk & accountabilities of personel
5. *Controls* – (whether control can address identified risks) & (Review key controls)
6. *Performance Measurement/Monitoring* – framework/ system is in place.

FIRE PAGES Auditor

Sample Areas of GRC for Review by Internal Auditors as per IIA:

S G E R I P E F A

1. Scope – Int. Auditor must improve GRC process.
2. Governance – to make appropriate recommendations to improve gov process.
3. Enterprise Ethics – evaluate, implementation design & effc. of Org ethics
4. Risk Management – evaluate effectiveness & improve Risk (M) process.
5. Interpretation – whether Risk (M) process are effective as per auditor.
6. Risk Management Process – gather info to support risk assessment.
7. Risk Exposures → org objectives, info, eff. of operations & process, Assets, laws
8. Evaluate Fraud & Fraud Risk – How org manage. Auditor to
9. Address Adequacy of Risk Management Process – Reframe from assessing adequacy, resp of Risk (M) &

check - CA

Specific Areas of Risk evaluated by Auditor are

Sample Areas of Review of Assessing & Managing Risks (MATMeTOM)

1. *Risk assessment methodology*
2. *Risk action plan & Timely reassessment.*
3. Different *types IT risks* (technology, security, continuity, regulatory, etc
4. *Quantitative* and/or *qualitative risk measurement*
5. Defined and communicated *risk tolerance profile*
6. Risk management *ownership* & *accountability* of Risk जिसकी जिम्मेदारी है
7. Root cause analyses & *risk mitigation measures*

Auditor

Evaluating and Assessing the System of Internal Controls as per COBIT 5:

COBIT 5 has specific process: "*MEA 02 Monitor, Evaluate and Assess the System of Internal Control*", which provides guidance on evaluating & assessing IC implemented in an org.

The objective of such a review is to:

i) *Continuously* ***monitor*** & evaluate **control** environment
ii) *Identify* ***management deficiencies*** & initiate improvement actions
iii) Plan, organize & maintain ***standards for internal control*** assessment

① Std, plans for IC
② Monitor, Evaluate
③ Assess deficiencies & improvements.

5 Mgmt

Key management practices for assessing & evaluating system of internal controls

1. *Perform Control Self-assessments* – evaluate completeness & effectiveness of (M) control over policy
2. *Ensure that assurance providers are independent & qualified* – Auditors
3. *Identify & Report Control Deficiencies*
4. *Scope assurance initiatives* – agree with (M)

IT Compliance Review

Some regulatory/legal requirements for GRC (Governance, Risk Management & Compliance) in an enterprise:

- ***Sarbanes Oxley Act*** (USA) -to protect investors by improving the accuracy & reliability of corporate disclosures.
- ***Clause 49 of SEBI***: mandates implementation of ERM & internal controls as appropriate for co.
- ***Information Technology Act***: It provides legal recognition for electronic records & mandates responsibilities for protecting information. identifies cyber-crimes & impose specific responsibilities on corporate.
- ***CARO:*** compulsory to report on Internal control & a separate annexure to audit report.
- ***PCAOB:*** In USA, the PCAOB has come out with detailed guidelines on Compliance by Auditors & co.s

IT Compliance in COBIT 5

- Cobit 5 **Management Domain** - *MEA03: Monitor, Evaluate & Assess - Compliance with External Requirements*
- **RACI Chart** *(Responsible, Accountable, Consulted or Informed)*
- *COBIT 5* ***Governance Domain***

(4) Key Management Practices of IT Compliance:

1. *Identify External Compliance Requirements* – understand which law are applicable to our orgn
2. *Optimize Response to External Requirements* – orgn will adjust & existing policy procedures as per appl laws.
3. *Confirm External Compliance* – Ensure existing policy comply with legal/Regm.
4. *Obtain Assurance of External Compliance* – Here we monitor, whether modified policies are properly followed. (& corrective actions to address compliance gaps)

(3) Key Metrics for Assessing IT Compliance Process:

I. ***Compliance with External Laws & Regulations***: metrics are-

- Cost of IT non-compliance
- No. of IT related non-compliance issues reported
- No. of contractual non-compliance issues
- compliance assessments. coverage

II. ***IT Compliance with Internal Policies:*** metrics are -

- No. of policy non-compliance
- % of stakeholders who understand policies
- % of policies supported by effective standards & practices
- Frequency of policies review & updates.

COBIT 5 – A GEIT Framework -Control Objectives for Information & Related Technology

- *It is a set of Globally accepted principles, practices, analytical tools & models that can be customized for biz of all size, sector & location.*
- COBIT: Developed by "Information System Audit and Control Association" (ISACA) USA
- Latest version: COBIT 5 *(April 2012)*
- COBIT5 structure: Five principles & seven enablers
- Process Reference Model – Governance domain & Management Domain

Need for Enterprise to Use COBIT 5

- *Provides good practice in Governance & management*
- *Create optimal value for the organization*
- Provides tools to understand, utilize, implement & direct IT related activities
- *Make more informed decisions*
- Can be used by all types and size of enterprises, including nonprofit and public sector

when cobit was Not there IT value ↓ Risk ↑ Benefit ↓

Benefits of COBIT5:

(Strategy) 1. Useful for Biz of **all Size**, type, sector
2. Achieve **objective** of Gov & Mgmt of IT
3.↑ **Increased value** from use of IT – balance between risk↓ & benefits↑ (Enterprise wide involvement)
4. Govern & manage IT in a **Holistic** manner taking full **End to End** Biz & IT functional areas
5.↓ ***Reduced IT related risks*** *& Ensure Compliance, continuity, security, privacy*
6.↑ ***Compliance with laws****, regl. policy, contractual agreements*
7. *Clear policy development &* ***Increase User satisfaction*** *with good practice of IT Mgmt*

COBIT 5 – Process Reference Model

- It defines & describes in detail – no. of gov & mgmt process of Enterprise IT in 2 main process domains. It incorporate both Risk IT (CIA) & Val IT (EE) frameworks.
- It provides a common reference model understandable by all users & managers
- It is a complete comprehensive model, but not the only possible process model. (customization)
- It provides framework for measuring & monitoring IT performance, providing IT assurance & integrating best management practices.

Complete cobit 5 enabler model includes total 37 gov & (M) processes providing end to end coverage of IT aligned with biz to achieve entrp obj

a. **Governance** → set direction, performance & compliance
Evaluate, Direct, Monitor (EDM 01 – EDM 05) – 5 processes.
SH needs & obj

b. **Management** (PBRM) – as per direction set by gov body
- Align, Plan, Organize (APO 01 – APO 13)
- Build, Acquire, implement (BAI 01 – BAI 10)
- Deliver, Service, Support (DSS 01 – DSS 06)
- Monitor, Evaluate, Assess (MEA 01 – MEA 03)

Components of COBIT 5 (PM is the model of FC Road)

1. Framework – IT gov obj ← link with → biz reqm
2. Process Description – 1 process ref model & common language for evl in orgn
3. Control objectives – control बताता है – it clear होता है (M) को – control reqm for each IT process
4. Management Guidelines – cobit gives guideline to (M) कि किसकी क्या Responsibility है – assign resp, measure performance, agree on obj.
5. Maturity models – what is reqd by Cobit (Maturity) & what u have (capability) → address gaps

Integrating/align COBIT with Other Frameworks

Many IT related std & best practice provides guidance on each subset of IT. Cobit is all in one

- GEIT → single overarching gov. & (M) Framework.
- ISO 27000
- ITIL
- Risk IT
- Val IT
- TOGAF (The Open Group Architecture Framework)
- ISO 38500

Align with:
→ Entrp policy, strategies, plans, audit Approaches
→ ERM framework
→ Existing entrp gov structure & processes

Customizing COBIT 5 as per Requirement/biz needs-

Cobit helps to meet following biz reqm –
1. Information security
2. Risk management
3. Governance & management of enterprise IT
4. Assurance activities
5. Legislative & regulatory compliance
6. Financial processing or CSR reporting

Five Principles of COBIT 5: (MEIS-Hai) (M15)

Principle 1: Meeting Stakeholder Needs ← create value for SH (लोग तुमसे क्या चाहते)
Principle 2: Covering the Enterprise End-to-End – It covers all functions / processes
Principle 3: Applying a Single Integrated Framework – comprehensive gov & (M)
Principle 4: Enabling a Holistic Approach – considers several interacting components
Principle 5: Separating Governance from Management

cobit < (M), gov

you'll get soln for every problem

Seven Enablers of COBIT 5: (P³ICSO) (M15)

शामिल करना, देने वाला – Factors which influence whether something will work: in cobit: Gov & (M) over Entrp IT

1. Principles, policies & frameworks – translate desired behaviour into guidance
2. Processes – activities to achieve certain obj
3. People, skills & competencies – काम करते हैं
4. Information – pervasive throughout the orgn
5.* Culture, ethics & behavior – संस्कृति
6. Services, infrastructure & applications (Technology) (ET)
7. Organizational structures – cobit की hierarchy से निर्णय लेने: not only top (M), in all key decision making entities in orgn.

Grow Risk (M) Compliance.

Using COBIT 5 Best practices for GRC: GRC program implementation requires the following steps:

1. Define what GRC requirements are applicable
2. Identify regulatory & compliance requirements
3. Review current GRC status
4. Determine most optimal approach
5. Setting out key parameters to measure of success Metrics
6. Using process oriented approach
7. Adapting global best practices, ~~and~~ cobit
8. Using uniform & structured approach which can be audited

Success of a GRC program can be measured by using the following goals and metrics: (4)

1. Reduction of redundant controls & related time to execute (Audit Test & Remediate) — Time ↓, Failure ↓, Exp ↓
2. Reduction in control failures in all key areas
3. Reduction of expenditure relating to legal, regulatory & review areas
4. Reduction in overall time required for audit — Audit Time ↓
5. Streamlining (improvement) of processes & automation of control & compliance measures — Improved process ↑
6. Timely reporting of regular compliance (issues) & Remediation measures — Reporting ↑
7. overall compliance status & key issues for senior management on a real time basis — compliance ↑

EDM
- KGI of GEIT
- KMP of Biz value from use of IT - (pg 4)
- KGP of Risk (M)

Key (M) practices
1. to Align IT strategy with biz strategy - (Pg - 4)
2. to evaluate whether biz value is derived from IT - (pg 4)
3. for implementing Risk (M) - pg - 7
4. - of IT compliance (cobit 5)
5. for assessing & evaluating IC system.

Key gov practice
1. which determine status of IT gov in entp: (IT gov) (pg 1) → who, what how, mechanism, monitor, exception.
2. GEIT (pg 1) → EDM
3. of Risk (M) (pg 7) EDM

Key Metrics
1. Measure biz value realised from use of IT in Biz (pg 4)
2. to monitor IT Risk (M) (pg 7)
3. for assessing IT compliance process. (pg 9)
4. to measure success of GRC program (pg 10)