Ch-1 : Concepts

Governance | IT Strategy | Internal Controls | IT Governance | Key Governance Practices | IT compliance Review

Governance

Basics

- ~~Dimensions~~
- **Benefits** (EDD's SHORTS)
  - Enterprise Objectives achieved
  - Desirable behaviour in use of IT encouraged
  - Desired business process implemented & integrated into enterprise
  - Strategically alligned decision making
  - Stability
  - Holistic IT Gov. framework
  - Overcoming limitations of organisat° structure
  - Improving customer business & internal relationships
  - Transparent decisions rights
  - Satisfaction customer, business & internal

Def°: A Governance system typically refers to all means & mechanisms that enable multiple stakeholders in an enterprise to have an organised mechanism for evaluating options, setting directions & monitoring compliance & performance to satisfy enterprise objectives

Enterprise Governance

- Dimensions:

Corporate Gov. (Conformance)	Business Gov. (Performance)
- Historic View	- Forward looking
- Focus on the regulatory req.	- Focus on strategy & value creation
- Monitored by Audit Committee	- No dedicated oversight mechanism

Points for CG

C-I-Cards.

- Compliances with relevant laws & regulations
- Internal Control Systems & IC Practices
- Clause 49 of LA
- Audit committee or its equivalent oversights the Board
- Risk Management
- Disclosure requirements
- Sarbanes Oxley Act ~~from~~ of US

IT Governance

[Def: IT Gov. refers to sys. in which directors of enterprise evaluate, direct & monitor IT mngt to ensure effectiveness, accountability & compliance of IT]

Key Practices to determine Status of IT Gov in ent.

INHIDER

- Who makes directing, controlling & executing decisions?
- What decision making mechanism are required?
- How are decisions Made?
- How exceptions handled?
- What info is req. to Make The decisions?
- How governance results monitored & improved?

CG & IT Gov

- Inseparable relationship.
- IT is key enabler of corp. business strategy.

Best Practices of Corp. Gov

I-C A-MIHIR

- ICS strong implemented
- Conflict of interest case-special monitoring of risk
- Assignment of responsibilities & decision making authority
- Mechanism for interaction & coop among Bod, Mngt & Auditors
- Incentives to act in appropriate manner
- Hierarchy of approvals
- Info flows appropriate internally & to public
- Risk Mngt functions.

Benefits of IT Gov

VET-COMPUSUMA (Meeting different objectives)

- Increased value delivered through enterprise IT
- IT becoming enabler for change rather than an inhibitor
- Transparency
- Compliances regulatory.
- Optimal ~~obtel~~ utilisation of IT resources
- Management of IT related risk
- Performance cost better.
- User satisfaction with IT services.
- Mitigation of IT related risk
- Agility in supporting business needs.

Ch-1 concepts

Governance

Governance of Ent. IT

Benefits of GEIT
I-C-DTC-BE
- Integrated approach
- Consistent approach
- Decisions IT related in line with strategy of ent
- Transparent
- Compliances regulatory
- Board Members governance requirements
- Enterprise Governance approach alligned with GEIT approach.

Key Governance Practices of GEIT
E/D/M 'Governance system'

Risk Management Strategies
AE-SIM
- Accept/Tolerate
- Eliminate/Terminate
- Share/Transfer
- Ignore/Train back
- Mitigate/Treat

Effective IT Gov. Structure

Components
- Enterprise Risk Mngt
- IT Risk Mngt

Definations (For RM)
- Asset
- Threat
- Vulnerability
- Attack
- Exposure
- Likelihood
- Availability
- Risk

Reasons for Gap between:
1. Degree of protection applied &
2. Need to protect systems

WIDE-UAE
- Widespread use of tech.
- Interconnectivity of sys.
- Devolution of mng & cont
- Elimination of distance, time & space as constraint
- Unevenness of tech. changes
- Attractiveness of unconventional electric attacks.
- External factors

Activities relating to Risk Management:
- Risk Assessment
  - Identification
  - Analysis
  - Prioritization
- Risk Mitigation Control
  - Reduction
  - Planning
  - Monitoring

Sources of risk
C-MINT-HELP
- Commercial Rel'n
- Management cont
- Individual act.
- Natural Events
- Technical Issue
- Human Behaviour
- Economic Circumstns
- Legal Relationships
- Political Circumst

Key Gov Practices of Risk Mngt: PTO
- Evaluate RM
- Direct RM
- Monitor RM

Key Mngt Practices of Risk Mngt
DAP-IDR
- Data collection
- Analyze Risk
- Maintain Risk Profile
- Info to articulate risk
- Define Risk Mngt Portfolio
- Response to Risk

Risk Mngt Metrics (Balanced Scorecard)
- % of critical bus. processes, IT service bus programs covered by RA
- No of significant IT related incidents Not identified in RM
- % of enterprise RA (Asst) incl. IT related
- Frequency of updating risk profile based on RA status.

IT Strategy

Types of Planning

Levels/Types of Managerial activities in ent.
- Strategic Planning
- Mngt Cont
- Operatn Cont.

- IT SP
- Others
  - IS Strategic Plan
  - Enterprise Strategy Plan (Corporate Plan)
  - IS Requirements Plan
  - IS Applications & Facilities Plan

Def. Str. Planning: Process of -
- deciding enterprise obj
- changes in them
- resources required from them
- policies to acquire, use & dispose those resources

- % of IT value drivers which are mapped to business value drivers

Key Mngt Practices to allign IT strategy with Enterprise Str.
1) Understand Enterprise direction
2) Define target IT capabilities
3) Conduct gap analysis
4) Define strategic plan & roadmap
5) Communicate IT Strategy & Direction

Metrics of above alignment
- % of enterprise strategy goals & requirements supported by IT str. goals
- Extent of stakeholder satisfn with scope of planned portfolio

Ch 1 concepts

Internal Controls

SEC's final rules us Security & Exg Comm

Co's Annual report to include 'IC report of Mngt' over IFR

IC report to contain
1) statement of mngt responsibility for estbl & maint & IC-FR
2) Identification of framework used to conduct eval" of IC-FR
3) Mngt assessment of effectiveness of IC-FR
+ disclose Material weakness
+ Not to conclude IC-FR is effective if 1 or more mat. weakness

4) Pub a/c firms attestation report on mngt assert of ICs over IFR

IC Components as per COSO

IC-MICR

Control Environment
Monitoring
Info & Comm"
Control Activities
Risk Assessment

IT Steering Committee

Key functions.

BAD-SCARE-PISS-RP

- Review budgets
- Approve & monitor key projects by measuring results (Return on Inv.)
- Decisions on key aspects of IT
- Size & scope of IT
- Conflicts to be resolved in IT deployment.
- Availability of link IT & its users ensure
- Reviews
- Enterprise goals - IT LTEST plans.
- Projects in all stages review.
- Implement" of security in enterprise
- Set priorities.
- Standards, policies & procedures.
- Report BOD regularly
- Performance of IT review.

Business Value from use of IT

To evaluate if BV obtained

Key Mngt Practices

- Evaluate Value Optimisation: Continually evaluate portfolio of IT inv. & assets. Considers if likelihood of objectives & realise at reasonable cost
- Direct VO: Direct Value Mngt - principles & practices to enable optimal value from IT invst. thru their eco. life
- Monitor VO: Goals, Metrics, issues, corrective action

Metrics for BV from IT use

- % of IT enabled inv. where benifits monitored full life.
- % IT services where expected benefits realised
- % of IT inv where expected benefits realised
- % of invst. business cases with clearly defined approved expected IT costs & benefits.
- % of IT services with
- Satisfn of stakeholders IT financial info

Key Governance Practices.

OF RISK MANAGEMENT

- Evaluate RM
Continually examine & judge effect of risk on current & future use of IT
Consider if risk appetite is appropriate.
- Direct RM
Direct RM activities to provide a reasonable assurance that IT RM activities are appropriate.
- Monitor RM.
Monitor key goals & Metrics & deviations & probs, etc. of RM

OF GEIT

- Evaluate Governance Sys.
Continually engage with stakeholders & judge the current & future design of GEIT
- Direct GS: Inform leadership & obtain support & commitment.
Guide processes & practices
- Monitor GS: Monitor effectiveness & performance of GEIT. Assess if operated effectively & provide appropriate oversight of IT

COBIT 5 Business framework.

Developed by Info Sys Audit & Control Association ISACA in 1996.

Components in COBIT

C-PM-FM

- Control objectives.
- Process description
- Maturity Models
- Framework
- Management Guidelines.

Benefits of COBIT 5

OH-CR-AP-GOBUS.

- Objectives enterprise
- Holistic Manner for gov. & mngt
- Compliance IT
- Compliance Legal & regulation
- Risk related to IT managed
- All sizes, etc enterprises can use.
- Privacy IT related
- Policy development.
- Good Practice for IT Mngt.
- Optimal value from IT
- Balance between benefits & risks
- User satisfaction.
- Security IT related.

Ch. 1: Concepts

COBIT 5 framework

Principles of COBIT 5
CAMES

1) Covering ent. end to end
2) Applying single integrated framework.
3) Meeting stakeholder needs
4) Enabling holistic approach
5) Seperating Governance & Mngt.

COBIT 5 includes a Process Reference Model.

Domains - 2 Main

Governance	Management
5 Processes.	4 sub domains
EDM01 to EDM05	APO 01 to APO 13 / BAI 01 to BAI 10 / DSS 01 to DSS 06 / MEA 01 to MEA 03
Evaluate, Direct & Monitor Practices	Align, Plan & Organize / Build, Acquire & Implement / Deliver, Support & Service / Monitor, Evaluate & Assess
EDM 5	APO 13 / BAI 10 / DSS 6 / MEA 3

Enablers of COBIT 5
COPPPIS ⑦

- Culture, Ethics & Behaviours
- Organisational Structures.
- Processes
- Principles, Policies & Frameworks.
- People, Skills & Competencies.
- Information
- Services, Applications & Infrastructure

[Def: Enablers are factors that individually & collectively influence whether something will work]

IT Compliance Review

Acts to protect Investors by corp disc

US	India
Sarbanes Oxley + oversight by PCAOB	• Cl. 49 LA • IT Act, 2000 + Guidance by ICAI to members & CARO, 03

Key Mngt Practices of IT compliance
IOCO

- Identify External Compliance Requirements.
- Optimize response to external requirements.
- Confirm External Compliance
- Obtain assurance of external compliance

IS Assurance

ML-CORP

Internal Audit activities to evaluate IT governance structure & practices:

1) Leadership
2) Organisational Structure
3) Processes
4) Risks
5) Controls
6) Performance Measurement/ Monitoring.

Prox

Metrics to assess compliance

→ With External laws
- Cost of IT non compliance (incl fees & settlements)
- No of IT related non comp issues reported or causing embarassment to public
- No of non comp related to contractual agreement with ITSP
- Coverage of compliance assessment

→ With Internal Policies.
- No. of incidents related to non compliance to policy
- % of stakeholders who understand policies
- % of ~~stakeholder~~ policies supported by standards & working practices.
- Frequency of policy review & update

IS Assurance

Sample areas for GRC review by Internal Auditors:

5G-E-MIME-FA

- Scope
- Governance
- Evaluate Ent. Ethics
- Risk Management
- Interpretation
- Risk Management Process
- ~~Adequacy of RM Process~~
- Risk Exposures Evaluation
- Fraud & Fraud Risk eval?
- ~~Interpretation~~
- ~~Enterprise Ethics~~
- Adequacy of RM Process

Sample areas for review of Assessing & Managing risk

Evaluate –

- RM ownership
- RM accountability
- Kinds of IT Risks
- Defined Risk Tolerance Profile
- Risk assessment Methodology
- Timely reassessment
- Root Cause analysis
- ~~Risk Mitigat~~ Risk measurement < Qty / Quality
- Risk Action Plan
- Risk Mitigation Measures

Key Mngt Practices for assessing & evaluating ICS

- Monitor IC
- ~~Perf~~ Review Business Process Controls Effectiveness
- Perform control self assessments.
- Identify & report Control deficiencies
- Ensure assurance providers are independant & qualified
- Plan assurance initiatives
- Scope ——u——
- Execute ——u——

PM Defn to learn

- Threat
- Risk
- Exposure
- Residual Risk
- Likelihood
- Attack
- Counter Measure