Concepts of Governance & Management of IS

Key Benefits of IT Governance	Improved management & mitigation of IT-related business risk; Improved transparency & understanding of IT's contr. to business; Improved compliance with relevant laws, regulations and policies; Improved agility (Responsiveness) in supporting business needs; Increased value delivered through enterprise IT; Increased user satisfaction with IT services;
	Better cost performance of IT; More optimal utilization of IT resources;
(N14+15)	IT becoming an Enabler for Change rather than an inhibitor.

Governance of Enterprise IT (GEIT)

> GEIT is a Sub-set of CG & facilitates implementation of a Framework of IS controls within an enterpris

> The Primary Objective of GEIT are to A&A the Requirement for GEIT & to put in place & maintain Effective Enabling S,P,P&P with clarity of responsibility & authority to achieve Entp's M,G&O.

Benefits		Ensures : Governance req for Board members are met Confirms : Compliance with Legal & Regulatory req. Ensures : IT-related decisions made in line with entp's S&O Ensures : IT-related process are overseen Effectively &Transparently
(RTP M-17)		Ensures : Consistent approach integrated&aligned with EG approach
Key Governance Practices (KGP)	EDM	Evaluate the Governance System Direct the Governance System Monitor the Governance System

KMP : To Evaluate ' Whether Business Value is derived from use of IT '

	EDM	Evaluate Value optimization	Continually Evaluate portfolio of IT enabled Investment (ITI) to achieve Entp. obj at reasonable cost
		Direct Value optimization	Direct Value mgt Principles & Practices to enable Optimal Value realization from ITI
(Pm Ex 2)		Monitor Value optimization	Monitor Key goals & metrics to determine the extent to which business is generating Expected Value from ITI

Key Metrics to Evaluate Benefits realized from ITI

	%	Percentage of ITI where benefit realization monitored through full economic life cycle;
		Percentage of ITI where claimed benefits met or exceeded;
		Percentage of IT services where expected benefits realized;
		Percentage of IT services with clearly defined & approved operational costs & expected benefits;
		Percentage of Investment business cases with clearly defined& approved expected IT related costs&benefits;
(RTP N-15)		Satisfaction survey of Key stakeholders regarding transparency, understanding&accuracy of IT financial info.

Internal Controls (IC) as per COSO

5 Inter-related Components	CRIM	Control activities	CA must be Developed to M,M&Reduce Risk asso. with EBP
		Control environment	CE must be Developed + Categorizing Criticality of EBP
		Risk assessment	CE must include an RA associated with EBP
		Info & Communication	Associated with CA are I&C system
			These enable Org. to Capture & Exchange info to manage & control its BP
(N-14)		Monitoring	IC process : Continuously Monitored with Modifications by Δ

KMP : Assessing & Evaluating ICS or KMP : Complying COBIT 5

(RTP : M-17)	PREMISE	Plan Assurance Initiatives	Based on Entp. obj & conformance obj.
		Perform Control Self-assessments	Encourage mgt to take positive ownership of control improv.
		Review BP Controls Effectiveness	Review : Operation of controls + Monitoring + Test evidence
		Ensure that assurance providers are independent & qualified	Independent from : the Function, Groups or Org in scope
		Monitor IC	Continuously monitor , Benchmark & Improve CE
		Identify & Report Control Deficiencies	Identify & Analyze underlying Root causes + Report to stkhldr.
		Scope assurance initiatives	Define & agree with Mgt. - Scope of AI
		Execute assurance initiatives	Executive the planned AI > Report on identified findinds.

Key Functions / Role of IT Steering Committee (ITSC)

(RTP : M-17)	Establish : Size & Scope of IT functions & set priorities within scope
	Ensure : Plans of IT dept ~ Enterprise goals & obj.
	Make decision on : All Key aspects of ITD & implementation
	Approve & Monitor : Key projects > Measuring results of projects : ROI
	Approve & Review : Major ITD projects in all their stages
	Approve & Review : Standards , policies & procedures
	Review : Status of IS plans & budgets & overall IT performance
	Facilitate : Implementation of IT security within an entp.
	Resolve : Conflicts in ITD
	Report : BOD on IT activities on regular basis.

3 Levels of Managerial activities

(N-15)	Strategic Planning	Process of deciding on Obj of entp & Resources used to attain Obj
	Management Control	Process : Managers assure - Resourced obtained & used E&E
	Operational Control	Process : Assuring that - Specific tasks are carried out E&E

KMP : Aligning IT strategy with Enterprise strategy { ITS ~ ES }

(M-15,16)	UA DC DC	Understand Entp. direction	Consider : Current Entp. env & BP + Entp. strategy & future obj
		Assess the Current E,C&P	Identify Issues currently experienced & Develop Recommendations
		Define the Target IT C	Based on understanding of Entp env & req.
		Conduct Gap analysis	Identify Gap between C & T env & consider alignment of assets
		Define Strategic plan & road map	How IT-related goals > contribute to Enterprise strategic goals
		Communicate ITS & Direction	To appr. stakeholders & users throughout entp.

Risk Management (RM)

Strategies :	T	Tolerate / Accept	If Minor risk > Consciously Accepting - COST of doing business is appropriate
		Terminate / Eliminate	Risk assos. with Technology > Replace Tech with more Robust
		Transfer / Share	With Trading partners&suppliers. Eg. : Outsourcing Infrastructure mgt
		Treat / Mitigate	Controls must be devised&implemented to PREVENT it form Manifesting
(RTP M-17)		Turn back	Prob or Impact Low > IGNORE risk
Metrics	RA	Percentage of Enterprise Risk Assessment(RA) including IT related risk	
		Percentage of CRITICAL BP , IT services & IT enabled business program COVERED by RA	
		Number of significant IT related incidents NOT identified by RA	
(N-15)		Frequency of UPDATING the risk Profile based on RA	
KMP		Collect data	Identify&Collect relevant data to enable effective IT related Risk Identification
		Analyze data	Develop useful Info to support Risk decisions
		Maintain a Risk Profile	Maintain an Inventory of known Risks & Risks attributes
		Articulate risk	Provide info - Current state > To stakeholders for appr. response
		Define a RM Action portfolio	Manage opportunities & Reduce Risk to an acceptable level
(M-15)		Respond to Risk	Respond in Timely manner with Effective measures to Limit Loss
KGP	EDM	Evaluate RM	Continually Examine : Effect of Risk on Current&Future USE of IT in entp.
		Direct RM	Direct : Establishment of RMP to provide reasonable ass. that IT RMP are appro. & Ensure : Actual IT risk not exceed Board's risk appetite
(RTP : N-16,M-15)		Monitor RM	Monitor : Key goals & metrics of RM process & Establish : How deviations will be I,T&R for correction

Control Objectives for Information and Related Technology (COBIT 5)

Components	5	Control Objective (CO)	Provides a Complete set of High-level req for Effective control of Each IT process
		Framework	Organize IT Governance obj & Good practice by IT
		Process Descriptions	A reference Process Model & common language for everyone in org.
		Mgt guidelines	Help : Assign resp. , Agree on obj. , Measure performance. etc

(RTP M-14)		Maturity model	Assess Maturity & capability per process & Helps to address gap
Benefits	5	Enable Enterprise - Achieving their Objective of Gov&Mgt of Enterprise IT	
		Enable - Clear Policy development & good Practice for IT mgt	
		Helps Enterprise : Managing IT related Risk + Ensures COMPLIANCE,security & privacy	
		Support : COMPLIANCE with relevant Laws , Regulations , Cont. agr. & Policies	
(RTP M-16)		Useful for Enterprise of ALL size : Commercial, Not for profit or Public sector.	
Principles	5	Meeting Stakeholder need	It provides ALL req process&other enables to Support Business Value Creation
		Covering Enterprise End-to-End	It integrates GEIT into Enterprise Governance + Cover ALL F&P
		Applying a SIF	It is a SIF as it Aligns with other LATEST relevant Standards&Framework
		Enabling Holistic approach	It defines a set of enablers to support Implementation of COMPREHENSIVE GEIT
(M-15)		Separating Governance from Mgt	It makes a Clear Distinction between Gov & Mgt
Enablers : 7	I COPS	Information	Pervasive throughout any org & inc ALL info produced&used by entp
		Culture, Ethics & Behavior	Very often Underestimated as a Success Factor in Gov&Mgt
		Organizational structure	OS are Key Decision Making entities in an enterprise
		Processes	Describes : Organized set of practices&activities to achieve certain obj.
		Principles, Policies & Framework	Vehicles to translate Desired behavior into Practical guidance
		People, Skills & Competencies	Req for Successful completion of ALL activities & making Correct decisions
(N-16)		Services, Infra & Application	Provides with IT processing & services.
KMP - IT Compliance with External Compliance (EC)	PPSPM	Identify EC requirement	Continually Identify & Monitor : Δ in International Laws,Reg & other ER
		Optimize response to ER	Review & Adjust : P,P,S,P&M to ensure that L,R&C req are addressed & comm.
		Confirm EC	Confirm EC : of P,P,S,P&M with L,R,C requirement
		Obtain Assurance of EC	Obtain & Report : Assurance of Compliance with P,P,S,P&M
(N-15)			

Sample Area of GRC for Review by Internal Auditor(IA)			
	GREASe	Governance	Must assess & Make recommendations for Improving Governance process
		RM	Must evaluate Effectiveness & make recommendation for Improving RMP
		RM process (RMP)	Gather info to Support this assessment during multiple engagements
		Evaluate Risk exposures	Relating to the Org's Governance, Operations & IS
		Evaluate Fraud & Fraud Risk	Must Evaluate Potential for Fraud occurrence > Managing Fraud Risk
		Evaluate Enterprise Ethics	D,I&E of Org's Ethics related objectives
		Address adequacy of RMP	Must address Risk consistent with Engagement's objectives & be alert
(RTP N-14)		Scope	Must Evaluate & make recom. for Impro. of G , RM & control processes

Sample Areas of Review of Assessing and Managing Risks

	Risk management ownership and accountability; Risk assessment methodology Risk action plan and Timely reassessment. Root cause analyses and risk mitigation measures; Different kinds of IT risks (technology, security, continuity, regulatory, etc.); Defined and communicated risk tolerance profile;
(Pm Ex 5)	Quantitative and/or qualitative risk measurement;

ISCA - The Conclusion

CONCLUSION - Ch 1

★ Yes , Conclusion Bcoz....

Why So ? What does it covers ?

★ Yes , it covers EVERYTHING :

- ✓ Practice Manual (including Exercise Questions)
- ✓ Past All RTPs (Including May-17)
- ✓ Past Examination Questions
- ✓ Mock Test papers

"OK! I got it the conclusion!"

★ **Spotlight -**

- ✓ "We would Daily Revise ISCA , HOW??
  - ➢ This Summary includes most EFFECTIVE Mnemonics
  - ➢ Along with Mnemonic "1 Line Must to Quote" has also to be learn.
  - ➢ 100% Module language!!!
- ✓ **Hello EveryBuddy :**
  - ➢ This is Kaival Shah , CA Finalist , just like u!
  - ➢ I am sharing this with an aim that it woud definitely , completely change your view about ISCA, from Being tuffest to Most Loved Subject!
  - ➢ And thus we Always score Highest in subject , we love the Most!

★ **Reading Technique :**

- ➢ Increase Learning Speed 3 times faster & if Revised daily - No chance of blink.
- ➢ I have grouped the Answer points in most EFFECTIVE sequence which are of similar nature . So that even in exam if 1 point clicks , we would be able to recall all points.

kaivalshah100@gmail.com

- ★ Quid pro Quo :
  - ✓ Do gift this to all your Friends!

"Help Others achieve their dream & You will achieve yours"

kaivalshah100@gmail.com