IT Governance

December 2009

Presented by: Tung Vo

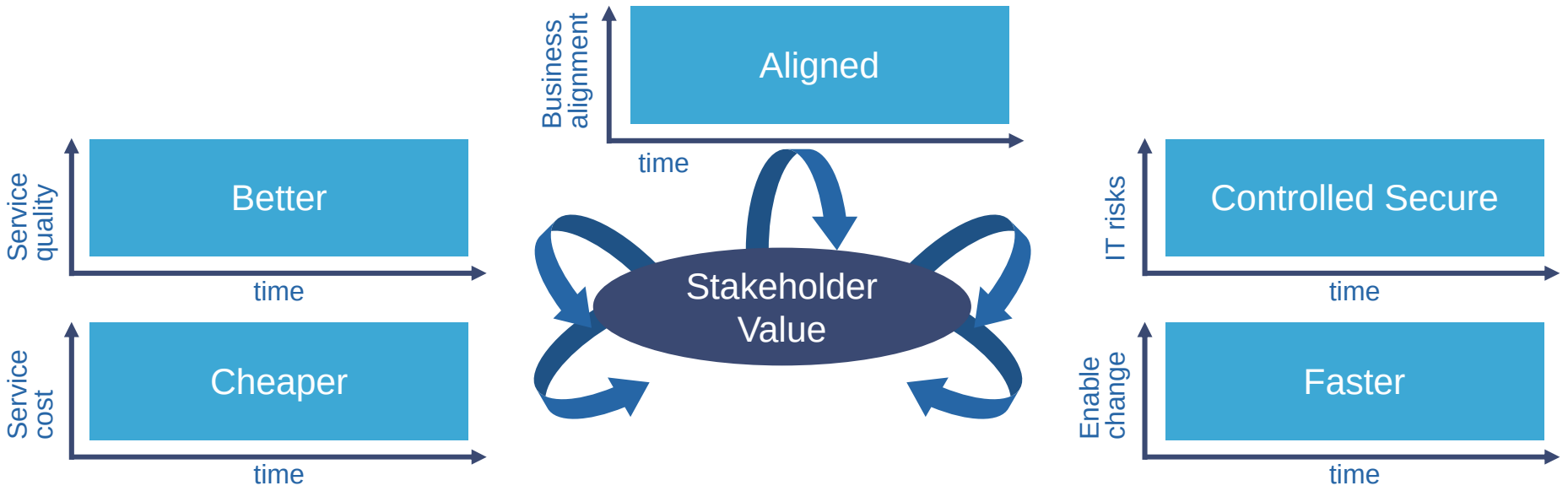
Agenda

- What is IT governance?
- Objectives of IT Govenance
- Distinction between IT Governance & IT Management
- Why is it so important?
- Relationship IT Governance & Risk
- COSO Framework for Enterprise Risk Management
- Mapping between IT Governance Objectives & COSO.
- CoBit IT Goverance Framework
- Definition: Policies, standards, process & procedures
- IT organization structures
- IT Governance – Performance Measures
- Critical success factors for of IT Governance
- IT Governance Summary.
- IT Governance Audit experience. Q & A

Definition of IT governance

- IT governance provides the framework and capacity for making and implementing decisions required to manage, control and monitor IT within the business

- A framework is required that defines these decisions, the involvement by various stakeholders, and the structures, processes, responsibilities and other mechanisms required to increase stakeholder value in a number of ways:



ITGI Definition of IT governance

"IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."

Reference : ITGI (IT Governance Institute) – www.itgi.org

Other definitions of IT governance

1. *IT governance can be defined as specifying decision rights and accountability framework to encourage desirable behavior in the use of IT* (Weill & Ross, 2004).
2. *IT governance is the structures and processes that ensure that IT supports the organization's mission. The purpose is to align IT with the enterprise, maximize the benefits of IT, use IT resources responsibly and manage IT risks.*
3. *A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk vs. return over IT and its processes.*
4. *IT governance is the system by which an organization's IT portfolio is directed and controlled. IT Governance describes (a) the distribution of decision-making rights and responsibilities among different stakeholders in the organization, and (b) the rules and procedures for making and monitoring decisions on strategic IT concerns (Peterson, 2004).*

The Objectives for IT governance are to ensure that:

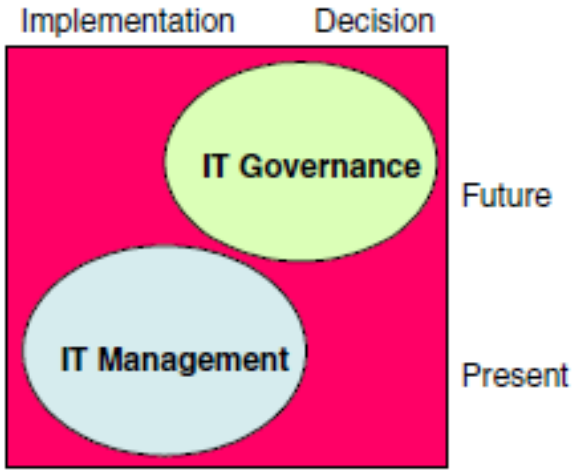
Strategic Alignment (includes Synergy Enablement & Shared Understanding)	The activities and functions of the IT organisation(s) are aligned to enable and support the objectives and priorities of the organisation. Synergies between IT initiatives are enabled and, where applicable, IT choices are in the best interest of the organisation as a whole vs. those of individual business units.
Value Delivery	IT delivers envisioned benefits against the strategy, costs are optimised, relevant best practices incorporated and that the value created for the organisation by its IT investments is maximised. There is a shared understanding, amongst all stakeholders, of how IT can add value to the organisation.
Risk Management	Compliance requirements are understood, there is an awareness of risk and the organisation's appetite for it and these residual risks are managed.
Resource Management	The optimal investment is made in IT and critical IT resources are responsibly, effectively and efficiently managed and used.
Performance Measurement	Performance is optimally tracked and measured and envisioned benefits are realised, including the implementation of strategic initiatives, resource utilisation and the delivery of IT services.

These objectives align with ITGI's Cobit 4.1

Distinction between IT management & IT Governance

The difference between IT management and IT governance is illustrated in the following figure:

Distinction between IT management and IT governance



What IT governance is NOT

Not just about Sarbanes Oxley or compliance issues

Not just about risks & controls

Not solely the responsibility of the CIO

No just about creating an IT steering committee

Not a “one-size-fits-all” framework

One size does not fit all

- It should be noted that, in light of the significant differences in each organisation's internal and external environment, there is no single IT governance model that is optimal.
- The key IT decisions, involvement of stakeholders, governance structures, processes and policies/principles/standards will be different for every organisation
- These governance arrangements also need to be flexible to change rapidly as factors in the internal and external environment changes.

Do any of these sound familiar with you? Are they drivers of the need for IT Governance ?

- The IT organisation is faced with dramatic change following a merger/acquisition
- The business is transforming and IT needs to follow/adapt in fast pace
- The business is unconvinced of IT's value and feels IT does not perform adequately.
- Outsourcing has been mandated without proper business case or without solving underlying problems, resulting in inadequate service.
- IT is a support function, and not capable to innovate and provide a competitive edge.
- The benefits of IT are not measured or cannot be demonstrated
- There is no adequate view or control over IT spending, and IT costs are perceived to be too high.
- The current IT architecture limits potential innovation capabilities and is not agile
- There is no good understanding of IT related risk and IT related risks are not managed
- The business does not understand how IT operates or what it can and cannot do within a certain timeframe
- IT does not have the right IT skills or resource numbers to deliver according to business expectations.

Why is IT governance important?

Profitability: Centre for Information Systems Research at MIT studied 256 enterprise in 23 countries

- Firms with above-average IT governance performance had more than 20% higher profitability than firms with poor governance → Conclusion: "Effective IT governance is single most important predictor of the value an organisation generates from IT"

Magnitude of IT expenditures…

- The average US organisation devoted 3.5% of their gross revenue to IT expenses in 2005*
- 2004 study of US and European firms found an average spend of 4.4% of revenue on IT**

…combined with some spectacular failures of some IT investments…

- ERP initiatives never completed
- One study estimates IT failure rates at over 70% of all IT projects***
- Nike reportedly lost more than $200m through difficulties in implementing its supply chain software

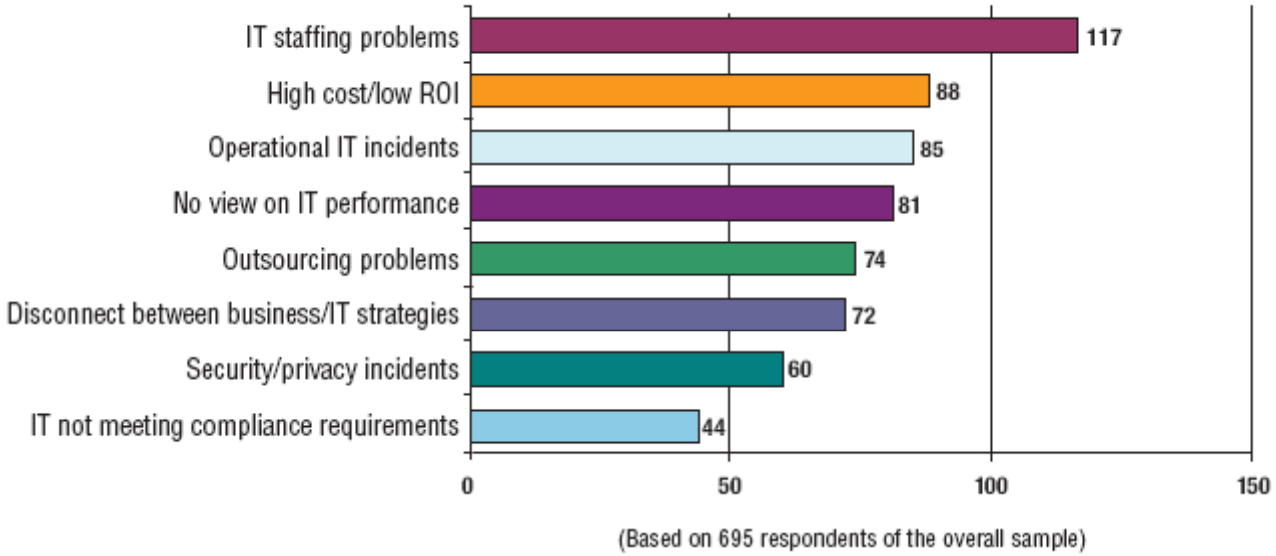
*Source: "US IT Spending and Staffing Survey", Gartner Research, 2005
**Source: "IT Spend Follows Organizational Structure", Forrester, 2004
***Source: "2001 Chaos Report", The Standard Group

Why is IT governance important? (cont'd)

An increasingly complicated IT sourcing environment

- Lack of skilled resources
- Outsourcing / Co-sourcing /Off-shoring
- Significant increase in the need for optimal oversight, control and management of IT

Figure 15—IT-related Problems in Last 12 Months (CPI)



Why is IT governance important? (cont'd)

Increasing impacts of IT incidents*…

- Cisco will lose $70 m in revenues if their systems are down for a day
- Amazon loses $600,000 an hour in revenue

IT is becoming a significant component for business innovation and competitiveness

- Supports standardised process activities, shared knowledge, instantaneous communications, and electronic interaction – the cornerstone for new business strategies
- IT needs to support fast changing business environment and new initiatives

*Source: "IT and the Board of Directors", HBR, October 2005

Why is IT governance important? (cont'd)

There are significant changes within the I(C)T environment and these are occurring at an ever-increasing rate

- Changes to the IT value chain
  - Many new application spans multiple businesses and functions
  - Increased interaction with customers and partners
- New I(C)T paradigms, including service oriented architectures (SOA), mobile technologies, process-to-software (P2S), convergence of IT and communications
- Increases in risk
  - Example: New channels for interaction that are emerging that poses significant security challenges, e.g. WLANs

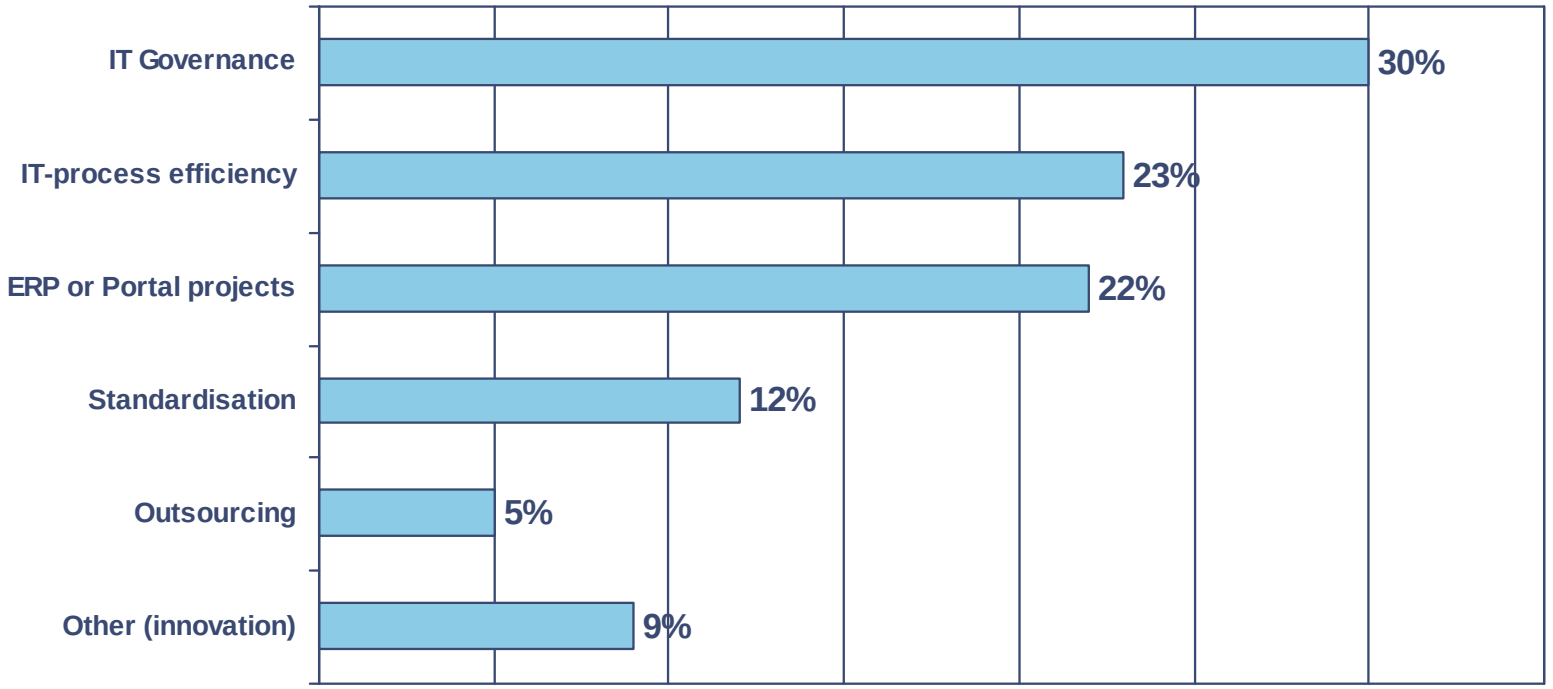
Why is IT governance important? (cont'd)

There is an need to meet increasing regulatory requirements for IT controls in certain industries and territories

- Organisations need to satisfy quality, fiduciary and security requirements for information as for all other assets
- Committee of Sponsoring Organisations of the Treadway Commission (COSO) defines widely accepted control framework for enterprise governance and risk management – also requires a framework for control over IT
- Sarbanes-Oxley, Basel II
- Industry specific regulations

Some more material to make the business case

- CIO's put IT Governance on the top of their own priority list for 2006-7

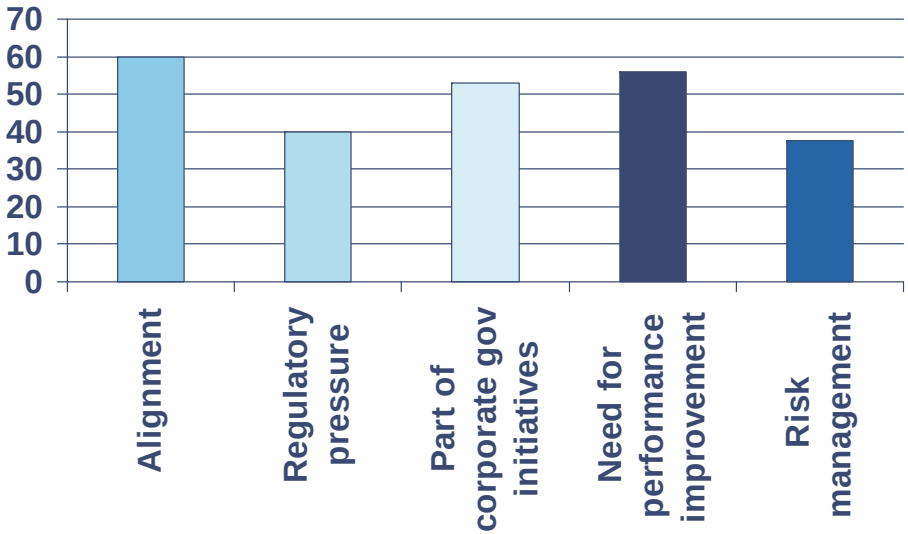


Source: Capgemini "European CIO Survey views on future IT delivery", 2006

Some more material to make the business case

CIO Survey conducted by PwC and ITGI in 2006 reported that:

60% of interviewees stated business-IT alignment as a significant driver for IT governance initiatives



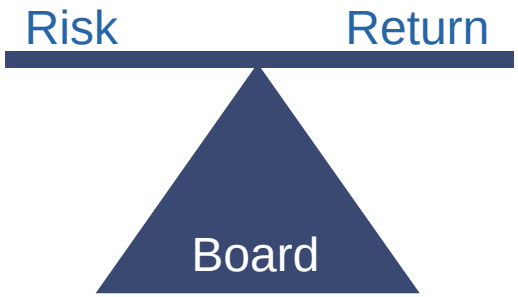
Correlation with the maturity of IT governance in an organisation

- Average maturity level on a scale of 0 – 5 for organisations that did not mention alignment as a driver: 2.3
- Average maturity level of those that did: 3.3

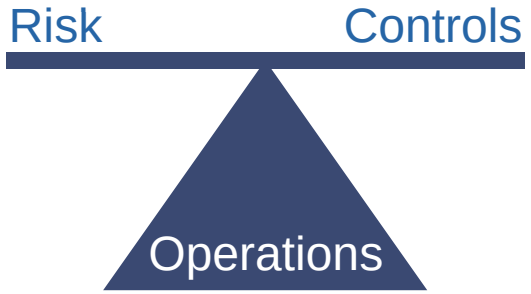
Relation between (IT) governance and risk

"Central to the requirement of enterprise governance is a clear relationship between the management of risk and the fulfillment of business objectives. Profits and growth are, in part, reward for successful risk taking"

(source: IFAC report, February 2004, Enterprise Governance, Getting the Balance Right)



"Mastering risk to create value"



"Getting the balance between conformance and performance right"

COSO: most accepted framework for Enterprise Risk Management

COSO Framework for Enterprise Risk Management

Monitoring

- Assessment of a control system's performance over time.
- Combination of ongoing and separate evaluation.
- Management and supervisory activities.
- Internal audit activities.

Control Activities

- Policies/procedures that ensure management directives are carried out.
- Range of activities including approvals, authorizations, verifications, recommendations, performance reviews, asset security and segregation of duties.

Information and Communication

- Pertinent information identified, captured and communicated in a timely manner.
- Access to internal and externally generated information.
- Flow of information that allows for successful control actions from instructions on responsibilities to summary of findings for management action.

Control Environment

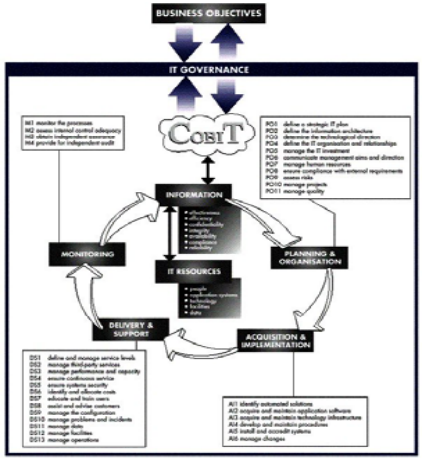
- Sets tone of organization influencing control consciousness of its people.
- Factors include integrity, ethical values, competence, authority, responsibility.
- Foundation for all other components of control.

Risk Assessment

- Risk assessment is the identification and analysis of relevant risks to achieving the entity's objectives-forming the basis for determining control activities.

IT Governance, CobiT and COSO

Mapping



IT process & controls framework

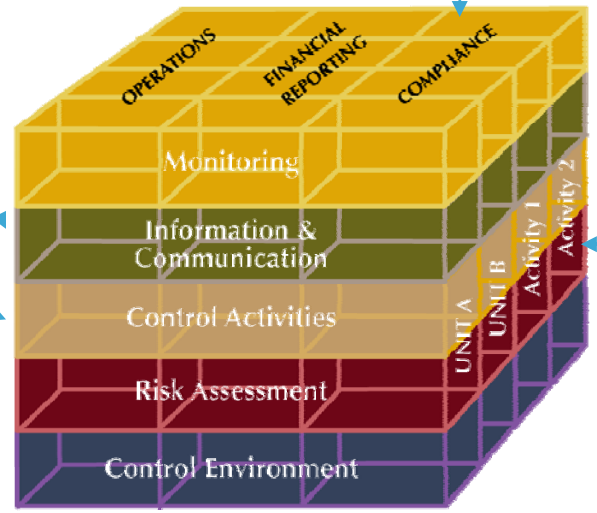
COSO Model for Enterprise Risk Management

Mapping of IT Governance objectives to COSO

Strategic alignment, with a focus on aligning with the business and collaborative solutions

Performance measurement, tracking project delivery and monitoring IT services

Resource management, optimising knowledge and IT infrastructure



Risk management, addressing the safeguarding of IT assets (including project investments), disaster recovery and continuity of operations

Value delivery, concentrating on optimising costs and proving the value of IT

CoBit 4.1 IT Governance Framework

Control Objectives for Information and related Technology **(COBIT®) provides good practices across a domain and process framework and presents activities in a manageable and logical structure.**

COBIT's good practices represent the consensus of experts. They are strongly focused more on control, less on execution.

These practices will help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong.

CoBit 4.1 IT Governance Framework

Figure — IT Governance Focus Areas

Strategic alignment : Ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.

Value delivery: executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.

Resource management ; optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.

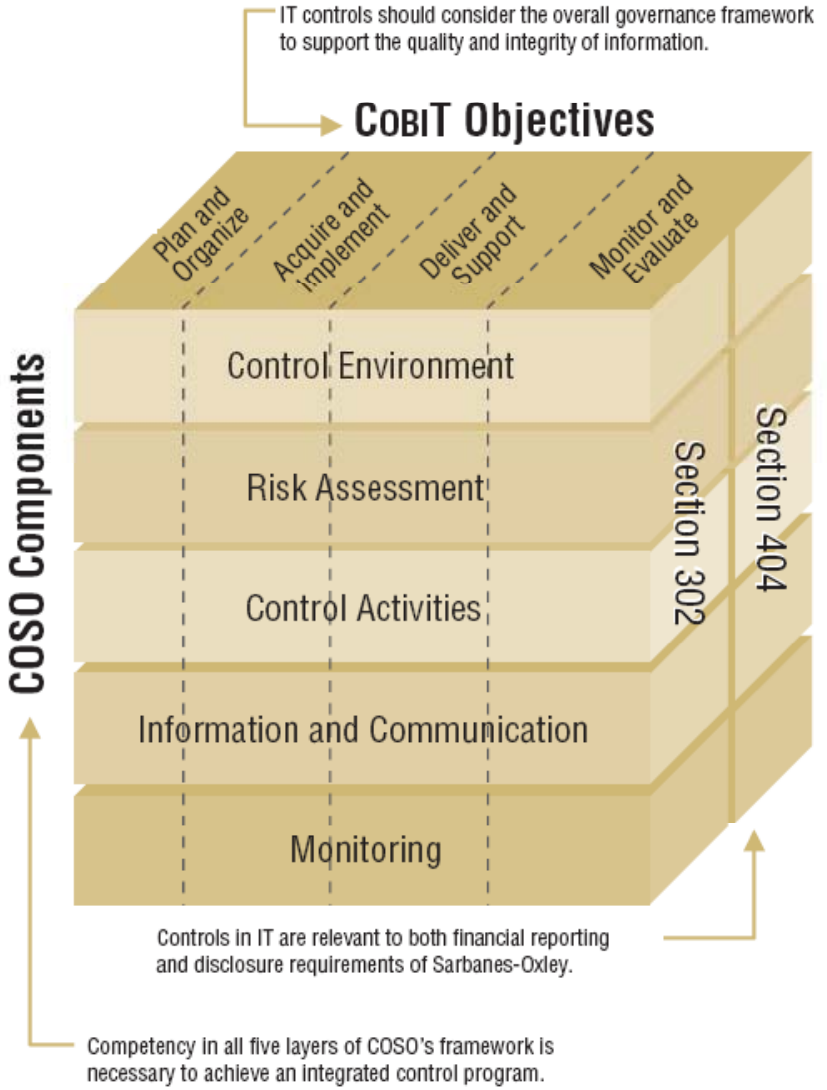
Risk management requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

COSO and CobiT Mapping

Cross-reference of COSO and COBIT Control Components

"An organization should have IT control competency in all five of the components COSO identified as essential for effective internal control"



CobiT focuses on what an organisation needs to do not how to do it

COSO and CobiT Mapping

Entity Level	Activity Level	CobiT IT Processes	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize (IT Environment)							
●		Define IT strategic planning.		●		●	●
		Define the information architecture.					
		Determine technological direction.					
●		Define the IT processes, organization and relationships.	●			●	●
		Manage the IT investment.					
●		Communicate management aims and direction.	●			●	
●		Manage IT human resources.	●			●	
●		Manage quality.	●		●	●	●
●		Assess and manage IT risks.		●			
		Manage projects.					
Acquire and Implement (Program Development and Program Change)							
		Identify automated solutions.					
	●	Acquire and maintain application software.			●		
	●	Acquire and maintain technology infrastructure.			●		
	●	Enable operation and use.			●	●	
		Procure IT resources.					
	●	Manage changes.		●	●		●
	●	Install and accredit solutions and changes.			●		

COSO and CobiT Mapping

Entity Level	Activity Level	CobiT IT Processes	COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Deliver and Support (Computer Operations and Access to Programs and Data)							
	●	Define and manage service levels.	●		●	●	●
	●	Manage third-party services.	●	●	●		●
		Manage performance and capacity.					
		Ensure continuous service.					
	●	Ensure systems security.			●	●	●
		Identify and allocate costs.					
●		Educate and train users.	●			●	
	●	Manage service desk and incidents.			●	●	●
	●	Manage the configuration.			●	●	
	●	Manage problems.			●	●	●
	●	Manage data.			●	●	
	●	Manage the physical environment.			●	●	
	●	Manage operations.			●	●	
Monitor and Evaluate (IT Environment)							
●		Monitor and evaluate IT performance.			●	●	●
●		Monitor and evaluate internal control.	●				●
●		Ensure regulatory compliance.			●	●	●
●		Provide IT governance.	●				●

IT governance – Policies and standards

Policies and standards are required to govern decision making

Definitions …..

- **Policies** A policy (or principle) sets direction and expectations on a subject. It is approved at the highest level of the organization, and designed to remain in effect regardless of changes in people, technology, or the mission of the organisation. The need for policies is driven by the business objectives, resource requirements, organisational risks, rules and legislation and the maturity level of the organisation. It also provides guidance for standards, processes and procedures, controls and structures.

- **Standards** describe the guidelines that should direct the practical implementation of policies. Standards establish a baseline for accomplishing procedures.

Definition of process and procedure

- **Process:** A sequence or order of activities, that also outlines the different decision points and functions responsible
- **Procedures:** detail the how of each of the activities within a certain process
- **The CobiT Framework** defines IT activities in a generic process model within the following four domains.