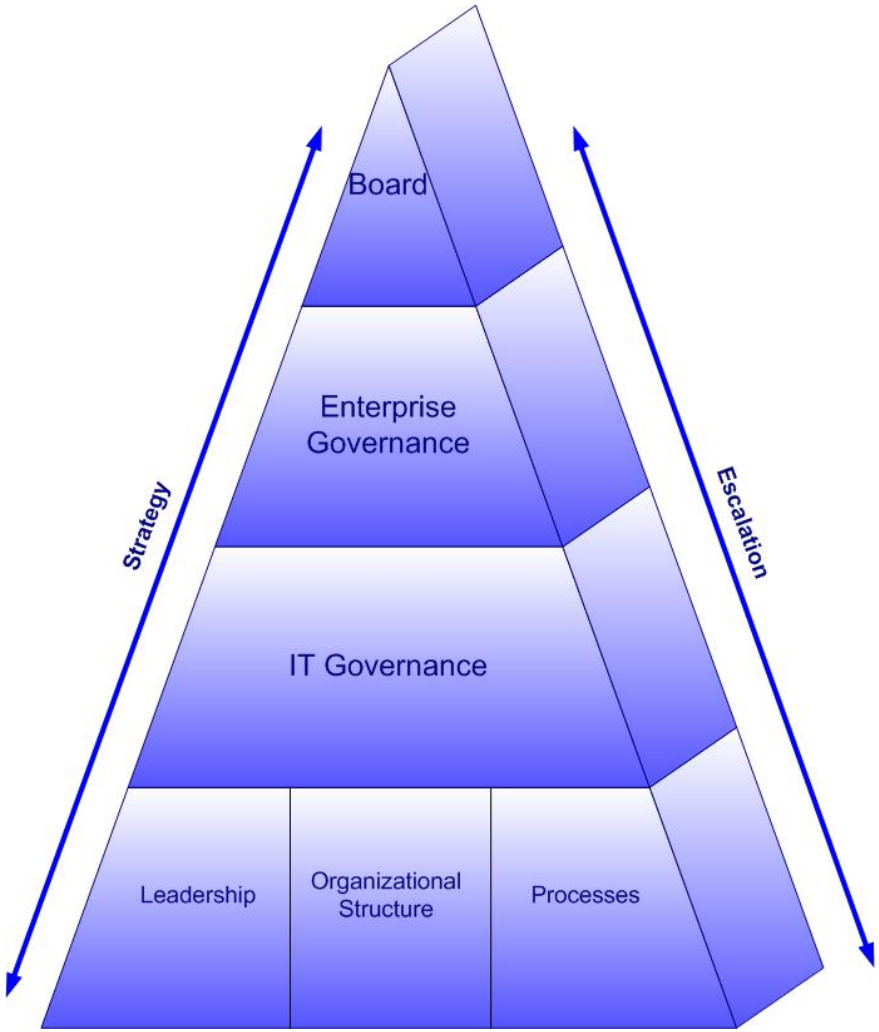
Achieve Risk Optimization with IT Governance Maturity Model

Lillibett Machado, MBA, CISM, CBCP

July 21, 2005

Enterprise Governance



Achieve Risk Optimization with IT Governance Maturity Model

Enterprise Governance

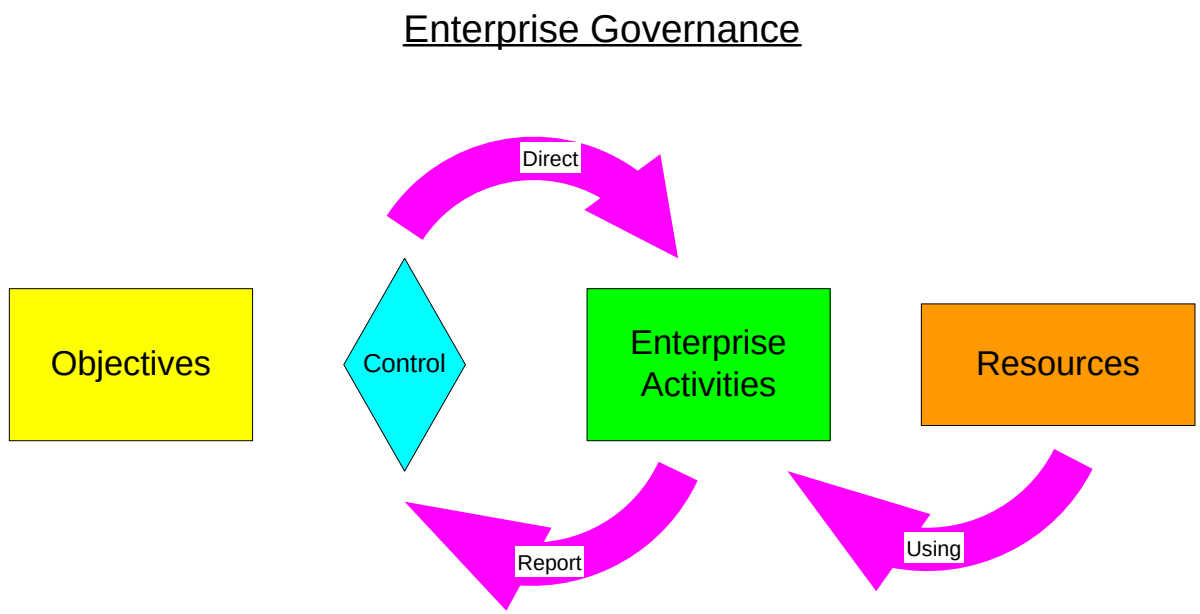
GOALS....

- Provide strategic directions
- Ensure objectives are achieved
- Ensure risks are defined and managed
- Verify that the enterprises' resources are used properly

Source: http://www.isaca.org

Enterprise Governance ...

- Enterprise governance is the system by which companies are directed and controlled and which drives and sets IT Governance.



Source: http://www.isaca.org

IT Governance - Definition

IT Governance .....

Structure

Relationships and Processes

Direct & Control

Achieve Enterprise Goals

Adding Value

Balancing Risk vs. Return

Over Information Technology

IT Governance ...

- IT governance is the responsibility of the Board of Directors and executive management.
- IT Governance is an integral part of enterprise governance and consists of the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.

Source: http://www.isaca.org

IT Governance

"To ensure IT sustain and extend the enterprises strategies and objectives"

Why.....

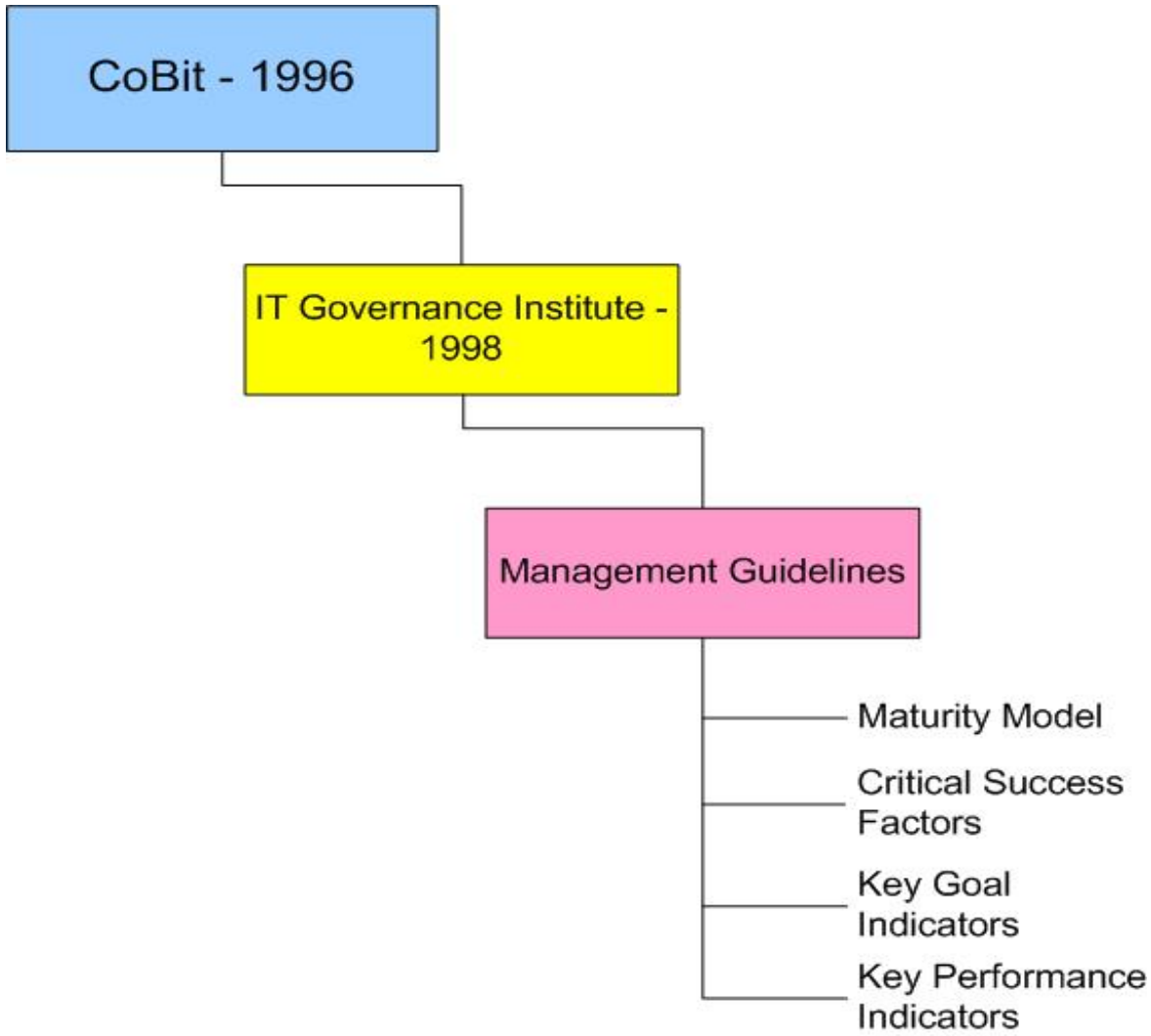
- To use IT's enabling capacity for new business models and changing business practices
- To achieve an appropriate return on IT's investment
- To manage ***technology risk***
- To maintain IT's ability to build knowledge
- To avoid IT failures that impact enterprise value and reputation

IT Governance – Environment

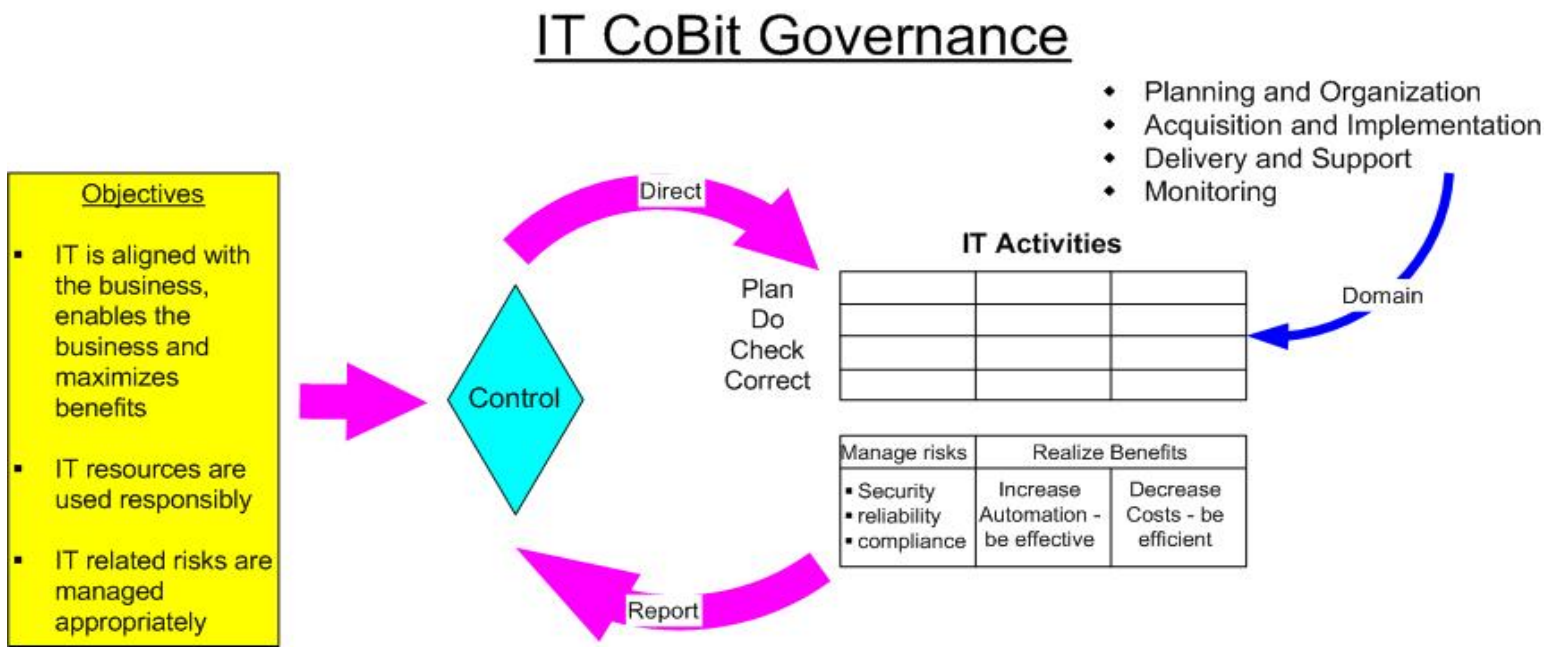
Challenges ....

- Stockholders value
- Missing vision and values
- Community and company ethics and culture
- Applicable laws, regulations and policies
- Industry practices

IT Governance - Evolution



IT CoBit Governance ...



Source: http://www.isaca.org

Risk Assessment

- Define threats and vulnerabilities
- Define inherent risk by determining likelihood and impact without any controls
- Determine control effectiveness
- Define mitigated risk by re-evaluating the likelihood and impact controls

Case Study

IT Risk Inventory / Control Analysis

IT Risk Inventory / Control Analysis

Objective

Develop a process that allows the discovery of optimal controls capable of reducing IT risk identified as “High”

IT Risk Inventory / Control Analysis

- Methodology
  - **Enhance CoBit Maturity Model** ranges from process to controls
  - Define critical success factors to enhance controls
  - Evaluate controls to determine expected impact & likelihood

Methodology

Enhanced **COBIT** Maturity Model for controls

Code	Name	Control Eff.	Description
0	Non-Existent	Weak	Control not available or ineffective
1	Initial		Control ad hoc with minimal effectiveness
2	Repeatable	Moderate	Control follows a regular pattern
3	Defined		Control are documented and communicated
4	Managed	Strong	Processes are monitored and measured
5	Optimized		Best practices are followed and automated

Methodology

- Define Critical Success Factors
  - Review & analyze current controls to determine deficiencies
  - Determine critical success factors to achieve risk optimization

Methodology

- Evaluate controls
  - Rate current controls effectiveness using the enhanced CoBit Maturity Model
  - Rate controls effectiveness assuming Critical Success Factors have been achieved
  - Re-evaluate risk impact & likelihood

Control Effectiveness Analysis – Sample Risks

- Inability to restore system in a timely manner
- **System recovery delays due to loss of accuracy and reliability of Technical Disaster Recovery (DRP)**
- Terminated employees retain access to system and network resources
- Project exceeds original budget in dollars and hours




		Inherent Risk												
Process	Risk	Impact	Likelihood	Inherent Risk Score	Controls	Control Effectiveness	Maturity Model Rating	Critical Success Factors	Scheduled Completion Date	Control Rating Objective	Impact	Likelihood	Mitigated Risk Score	
Business Continuity	System recovery delays due to loss of accuracy and reliability of Technical Disaster Recovery Plans (DRP)	3	4	12		Moderate					3	3	9	High
					Enforce standard operating procedures (SOP), such as Maintenance Schedule, Validation and Testing, and Training		3.0	Technology Managers must also enforce SOP Access to DR Site. Awareness should be given to Technology Managers on the need to enforce the SOP.	7/23/2002	4.0				
					Quarterly review and approval of DRPs by users and CBC		2.0	Technology Managers should review every change control to determine if the change will impact the Technology Recovery Plan for the group	12/12/2002	3.0				
					CBC involvement in technology strategy definition before project kick off		1.0	CBC Representative is included in monthly review meeting of technical projects	7/15/2002	3.0				
					CBC involvement in technology DR design meetings when determining DR strategy		1.0	CBC should participate in the design of the Recovery Strategy with IT	7/15/2002	3.0				
					Internal/External Audit reviews		4.0			4.0				
					Control Average Value		**2.2**			**3.4**				
					Score Changes after achieving Success Factors						3	2	6	Medium
								Awareness Program already planned for 2002 on BC methodology and SOP's which will be supported by Corporate Training. IT Quarterly Recovery Plan quality and the participation on technology meetings has increased due to the transfer of a trained Technology System Engineer to a BC Planner position. The strong technical skills added to the BC resources has						
					Control Effectiveness Change:	Moderate		SOPs will be updated and IT personnel trained by 1/31/04. Change Control compliance at hot site will be included as a responsibility of IT Managers. At present BC is activily participating on IT projects providing DR reliable strategies and recovery procedures since 11/30/02.	1/31/2003		2	3	6	Medium

Sample Analysis Spreadsheet

References

- http://www.isaca.org
- http://www.drii.org
- http://www.drj.com/
- http://www.contingencyplanning.com/
- http://www.continuityinsights.com/
- http://www.thebci.org/
- http://www.availability.sungard.com/
- http://www.drs.net/

Contact Information

Lillibett Machado, MBA, CISM, CBCP, ITIL-BSM

Telephone: 713-232-6323

e-mail: Lillibett.Machado@amegybank.com

Thank You...