

Overview of IT Governance and COBIT

A.Rafeq
ISACA, Bangkok chapter
COBIT Workshop
21 July 2006

IT Governance

- Board and senior management
- IT Governance – focus on using IT for business objectives for competitive and strategic advantage
- Why? IT is a major investment
- IT is a major expenditure

Five Focus areas

1. **Strategic alignment:** Align IT with business
2. **Value Delivery:** Ensuring value out of IT investments
3. **Risk Management:** Mitigating risks
4. **Resource Management:** Optimum utilisation of IT resources
5. **Performance measurement:** goals and metrics

COBIT Components

- Executive Overview: Primarily for senior management, provides brief overview of principles/philosophy of IT Governance and COBIT
- Framework: explanation of Cobit Principles and concept
- Control Objectives: Controls and what is the objective of controls – 209
- Management Guidelines
 - Input-output matrix: Process owner – document
 - RACI Matrix: Establishing accountability across all the key IT activities of that process – CSF
 - Goals and Metrics: Activity goals, Process Goals, IT Goals, P-KGI, IT KGI
 - Maturity Model: Assessing current status of maturity of the process

Maturity model

0: No process exist

1: Initial/ad-hoc

2: Repeatable

3: Defined - documented

4: Managed – ensure usage of documentation and monitoring it's implementation

5: Optimised: automated process of managing and continuous improvement

COBIT

- Domains – IT processes:
 1. Plan and Organise - 10
 2. Acquire and Implement - 7
 3. Deliver and Support - 13
 4. Monitor and Evaluate - 4
- Control Objectives: 209
- Control Practices still version 3: ~2000

Cobit Usage

- **Two Approaches:** Big Bang, Gradual
- **COBIT Use:**
 - Understand what each IT process
 - Understand Framework – linkage with business requirements
 - Control Objectives: 4 to 10
 - Management guidelines: Maturity model, IO, RACI & GM

Cobit cube

- Domains, ITP, activities
- IT resources: 4: Infrastructure, Applications, Information, people
- Information Criteria: Business requirements of information:
 - **Quality:** Effectiveness, Efficiency
 - **Fiduciary:** Compliance, Reliability
 - **Security:** CIA

Controls, Control Objectives and Risks

- Control:
 - Policies, Procedures, Practices & Organisation Structure
 - Designed
 - Assurance – reasonable
 - BO are achieved
 - Undesired events are prevented or detected and corrected
- Control Objectives: Reason, purpose or objective of controls
- Control equation:
 - $C = R$: Acceptable
 - $C < R$: Control weakness, residual risk, exposure – potential loss
 - $C > R$: extra cost
- Risk: PO9: IT process on risk assessment
 - CO: Negative,
 - MG: Maturity level lower: risk
 - IO = Input output matrix – documents not prepared

Cobit – 5 Techniques

1. IT Process
2. Information criteria
3. IT resources
4. BG – ITG – ITP
5. Control F: Find,
6. COBIT Online: Themes
7. Customise: Control R: find and replace

Use COBIT?

- What is the objective of COBIT use:
 - Controls: Control Objectives
 - Performance Management; MG
 - Combination of both
- Identify IT process
- Select Control Objectives
- Customise as required
- Add BP/Technology controls as required

Risk and Return - Balance

- Balancing
 - Risk
 - Return
 - Optimum level of investment for controls
- COBIT:
 - Benchmark, guideline, standard
 - Collection of best practices
 - GAAP: Consensus of experts

COBIT Advantage

- Common means of communication across stakeholders
- Three distinct audience
 - Management
 - BP Owners
 - Auditors

COBIT characteristics

- Generic
- One size fits all – no, need to customise
- Only a guidelines – don't take it as etched in stone
- COBIT: What is the benefit, what problem can be solved – bottom-line for using COBIT

PDCA

- Plan
 - Do
 - Check
 - Act
-
- (Plan, Build, Run) + monitor

Unique Differentiator

- IT Governance Model
- Macro - umbrella standard
- Integrate other standards as required