IT Governance

Arrianto Mukti Wibowo,
M.Sc., CISA
Agenda

• What is IT Governance?
• Why important?
• Whom does it concern?
• What does IT Governance cover?
• What questions should be asked?
• COBIT & IT Governance
• Cases
What is IT Governance?
What is IT Governance?

• IT governance is the responsibility of the board of directors (*komisaris*) 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.
Cont’d

• Sustaining the current business and growing the business are certainly stakeholder expectations and can be achieved only with adequate governance of the enterprise’s IT.

• Also critical to the success of these structures and processes is effective communication among all parties based on constructive relationships, a common language and a shared commitment to addressing the issues.
IT Governance vs IT Management

IT Governance concentrates on performing and transforming IT to meet present and future demands of business.

IT Governance is organization specific, and direct control over IT can not be delegated to the market.

(Peterson, 2003)

IT Management is focused on the internal effectiveness supply of IT services and products, and also the management of IT operations.

(Time Orientation)

Business Orientation

External

Internal

Present

Future
IT Governance Framework

Set Objectives
- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT-related risks are managed appropriately

Provide Direction

Compare

Measure Performance

IT Activities
- Increase automation (make the business effective)
- Decrease cost (make the enterprise efficient)
- Manage risks (security, reliability and compliance)
Peterson Model (2003) of IT Governance Structures, Process & Relationship Mechanisms
Why is it important?
Why IT is important in the first place?

- There is a shift of the meaning of ‘asset’. Nowadays, intangible asset (information, knowledge, expertise, reputation, trust, customer) is an important part for company’s *sustainable* competitive advantage.
  - And, many of these assets rely on IT!
- Furthermore, IT is not just seen as business enabler. Service delivery in the financial world is entirely dependent on IT and requires system reliability and information integrity. No banking transaction can be executed without the IT infrastructure.
Why IT Governance?

• IT requires huge investments.
• But few (top executives) knows how to make IT Dept accountable for delivering value!
• They need some special ‘governing tool’ to measure IT, because IT is considered ‘too technical’.
• But too important to ignore!
• And yet, IT itself introduces new risk that has to be managed properly.
Pressures for IT Governance
AS-8015 Good Corporate Governance for ICT
So what are the pressures & drivers?

1. Accountability for bringing business value, as IT investment is huge.
2. To minimize risk, as banking operations heavily depend on IT
3. Pressures from regulators
   - Bank Indonesia
   - Kementrian BUMN (Kepmen no.117 tahun 2003 tentang GCG)
   - Bapepam-LK
4. Agreement with business partner:
   - Card brand
   - Banking network
5. Pressures from customer for better service. If not taken seriously, customer may switch to other banks!
6. Technological changes $\rightarrow$ introduce new opportunity or new risk!
7. Organization’s GCG programme may require all areas to be governed properly.
### IT Gov & GCG Questions

<table>
<thead>
<tr>
<th>Corporate Governance questions</th>
<th>IT Governance questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do suppliers of finance get managers to return some of the profits to them?</td>
<td>How does top management get their CIO and IT organisation to return some business value to them?</td>
</tr>
<tr>
<td>How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects?</td>
<td>How does top management make sure that their CIO and IT organisations do not steal the capital they supply or invest in bad projects?</td>
</tr>
<tr>
<td>How do suppliers of finance control managers?</td>
<td>How does top management control their CIO and IT organisation?</td>
</tr>
</tbody>
</table>
Whom does it concern?
All Levels...!
Cascaded objectives

- Business Unit Scorecard
- Corporate Scorecard
- IT Scorecard

BU Managers → IT Managers → BoD, C-level executives
Komisaris, Direktur

Provide information for decision making
Board of Directors

- What BoD (komisaris) can do:
  1. Set direction & the expected return on “IT”
  2. Obtain IT assurance through IT audit
  3. Monitoring how management determines what IT resources are needed to achieve strategic objectives
  4. Ensuring major IT development projects are aligned with the business strategy and have an approved business case which clearly demonstrate value and how it will be measured
  5. Ensures proper IT risk management are in place
  6. Ensure culture of openness & transparency of risks!
  7. And others… (see Board IT Governance Tool Kit)

- Usually assisted by *IT Strategy Committee* (ITGI best practice, however names are sometimes different among organizations).
Senior Management / Top Executives

• What they should do:
  – Cascade strategy, policies and goals
  – Provide organisational structures
  – Embed clear accountabilities
  – Measure performance
  – Focus on core business competencies IT must support
  – Focus on important IT processes
  – Focus on core IT competencies
  – Create a flexible and adaptive enterprise
  – Strengthen value delivery
  – Focus on the optimisation of IT costs
  – Have clear external sourcing strategies

• Assisted by IT Steering Committee
What does IT Governance cover?
Focus Area of IT Governance
Life Cycle
Strategic Alignment Model

• Diperkenalkan oleh Henderson & Venkatraman (1993)
• Berguna untuk landasan filosofi berpikir
• Ide dasarnya pada:
  – *strategic fit*: bagaimana strategi TI harus dibahasakan dalam *domain external* (*how the firm is positioned in the IT marketplace*) dan *domain internal* (*how IT infrastructure should be configered*)
  – *functional integration*: berbicara bagaimana ranah TI akan mempengaruhi ranah bisnis (*business domain*)
External IT Domain Decisions

• IT Scope
  – Hal-hal dari TI yang mendukung insiatif strategi bisnis atau memungkinkan munculnya strategi bisnis yang baru

• Systemic Competencies
  – Yakni yang merupakan karakteristi IT strategy, misalnya: cost-performance level dan masalah flexibility sehingga perusahaan bisa responsif

• IT Governance
  – Pilihan mekanisme yang dipergunakan agar perusahaan memiliki kompetensi yang dibutuhkan
Internal Domain Decisions

• IT Architecture
• IT Process (mis: system development maintenance)
• IT Skills, terkait masalah rekrutimen, pelatihan dan pengembangan SDM TI

• Problemnya, manager IT kebanyakan hanya memikirkan *internal domain decisions*!
Functional Integration

• Berbicara bagaimana ranah TI akan mempengaruhi ranah bisnis (*business domain*)

• Strategic integration adalah hubungan antara business strategy dengan IT strategy

• Operational integration adalah hubungan antara infrastruktur/proses dalam organisasi dengan infrastruktur/proses TI
Strategic Alignment Model Diagram
Strategic Alignment Domains

- Henderson & Venkatraman mengatakan ada 4 model bagaimana alignment tersebut dapat dicapai:
  1. Strategic execution alignment
  2. Technology transformation alignment
  3. Competitive potential alignment
  4. Service level alignment
Strategic Alignment Domains Diagram

- **Strategy execution alignment**
  - Business strategy
  - Organizational infrastructure
  - IT infrastructure

- **Technology transformation alignment**
  - Business strategy
  - IT strategy
  - IT infrastructure

- **Competitive potential alignment**
  - Business strategy
  - Organizational infrastructure
  - IT strategy

- **Service level alignment**
  - IT strategy
  - Organizational infrastructure
  - IT infrastructure
Strategic Alignment Types

• Strategic Execution:
  – Bersifat hierarkis dan paling umum, bahwa strategi bisnis menentukan desain organisasi dan juga desain infrastruktur TI-nya.

• Technology Transformation:
  – Juga start dari business strategy, tetapi fokus pada implementasi strategi TI yang tepat, baru pada infrastruktur dan proses
Strategic Alignment Types

• Competitive potential
  – Paradigma ini memungkinkan adaptasi atau munculnya suatu strategi bisnis karena munculnya kapabilitas baru dari TI.

• Service Level perspective
  – Cara pandang ini lebih berpikir pada bagaimana cara membuat unit/organisasi TI yang menyediakan layanan prima.
Six Step Process for Alignment
(Luftman & Brier, 1999)

- Set the goals and establish a team
- Understand the business-IT linkage
- Analyse and prioritise gaps
- Specify the actions (project management)
- Choose and evaluate success criteria
- Sustain alignment
Vertical & Horizontal Alignment
Guldentops (2003)

- Inclusion of all parties
- Clear responsibilities
- Integration diff. Strategies
- Sign-off on scorecard
- Co-responsibility
- Practical business involvement
- Service levels & performance measurement

- Cascading objectives and strategy
- Strongly communicated & translated for each layer
- Few but precise performance measures directly and demonstrably linked to strategy
## Enablers & Inhibitors of Strategic Alignment

<table>
<thead>
<tr>
<th>ENABLERS</th>
<th>INHIBITORS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior executive support for IT</td>
<td>IT/business lack close relationships</td>
</tr>
<tr>
<td>IT involved in strategy development</td>
<td>IT does not prioritise well</td>
</tr>
<tr>
<td>IT understands the business</td>
<td>IT fails to meet commitments</td>
</tr>
<tr>
<td>Business-IT partnerships</td>
<td>IT does not understand the business</td>
</tr>
<tr>
<td>Well-prioritised IT projects</td>
<td>Senior executives do not support IT</td>
</tr>
<tr>
<td>IT demonstrates leadership</td>
<td>IT management lack leadership</td>
</tr>
</tbody>
</table>
IT Strategy drives IT Process

- Different strategy, different important process (e.g. mining vs banking)
Value of IT at different levels of organization (Weill & Broadbent, 1998)

• Manager dan user pada tingkat yang berbeda akan mempersepsikan manfaat/nilai/value dari TI yang berbeda.
• Implementasi TI yang strategic akan memiliki dampak yang besar dalam semua level dari business value hierarchy.
• Pengukuran investasi TI akan mudah di hirarki yang bawah ketimbang yang di atas!
Value of IT at different levels of organization (Weill & Broadbent, 1998)

Sample Measures
- Revenue growth
- Return on assets
- Revenue per employee
- Time to bring a new product to market
- Sales from new product
- Product or service quality
- Implementation time: new application
- Implementation cost: new application
- Infrastructure availability
- Cost per transaction
- Cost per workstation

Business Value Delivered
- Business Unit Financial
- Business Unit Operational
- Business Unit IT Applications
- Firm-wide IT Infrastructure

Measure performance
Manage cost

Time for Business Impact
Risk Management

- Risk management dapat dipandang sebagai pasangan dari value creation, yakni *business value preservation*.
- ISO 27001 Information Security Management Systems

<table>
<thead>
<tr>
<th>No</th>
<th>Assets</th>
<th>Vulnerabilities</th>
<th>Threats</th>
<th>Outcome</th>
<th>Impact Value</th>
<th>Likelihood</th>
<th>Current Control</th>
<th>Current Risk Control</th>
<th>Inherent Risk</th>
<th>Control Objective</th>
<th>Additional Control</th>
<th>Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Customer Database Documentation</td>
<td>□ Data saved in storage disk  □ Connected to the network  □ Put on the improper place</td>
<td>□ people using access to network  □ people using physically access storage damage</td>
<td>□ disclosure  □ modification  □ loss/destruction</td>
<td>5</td>
<td>2</td>
<td>OKK08B1,OKK08B2,OKK08B3,OKK10B1,OKK10B2,OKK12B1,OKK14B1,OKK14B3</td>
<td>3</td>
<td>30</td>
<td>OKK08A, OKK10A, OKK12A, OKK14A</td>
<td>Acceptable</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>User Access Control Database Documentation</td>
<td>□ Data saved in storage disk  □ Connected to the network  □ Put on the improper place</td>
<td>□ people using access to network  □ people using physically access storage damage</td>
<td>□ disclosure  □ modification  □ loss/destruction</td>
<td>4</td>
<td>2</td>
<td>OKK08B1,OKK08B2,OKK08B3,OKK10B1,OKK10B2,OKK12B1,OKK14B1</td>
<td>3</td>
<td>24</td>
<td>OKK08A, OKK10A, OKK12A, OKK14A</td>
<td>Acceptable</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Asset Information (Vendor, Support, Life time, contracts, licences)</td>
<td>□ Data saved in storage disk  □ Connected to the network  □ Put on the improper place</td>
<td>□ people using access to network  □ people using physically access storage damage</td>
<td>□ disclosure  □ modification  □ loss/destruction</td>
<td>3</td>
<td>2</td>
<td>OKK08B1,OKK08B2,OKK08B3,OKK10B1,OKK10B2,OKK12B1,OKK14B1,OKK14B2,OKK14B3</td>
<td>3</td>
<td>18</td>
<td>OKK08A, OKK10A, OKK12A, OKK14A</td>
<td>Acceptable</td>
<td></td>
</tr>
</tbody>
</table>
# Performance Measure

<table>
<thead>
<tr>
<th>Perspective</th>
<th>Objective</th>
<th>Example Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate</td>
<td>• Business/IT alignment</td>
<td>• Operational budget approval</td>
</tr>
<tr>
<td></td>
<td>• Value delivery</td>
<td>• Business unit performance</td>
</tr>
<tr>
<td></td>
<td>• Cost management</td>
<td>• Attainment of expense and recovery targets</td>
</tr>
<tr>
<td></td>
<td>• Risk management</td>
<td>• Results of internal audits</td>
</tr>
<tr>
<td></td>
<td>• Intercompany synergy</td>
<td>• Single system solutions</td>
</tr>
<tr>
<td>Customer</td>
<td>• Customer satisfaction</td>
<td>• Business unit survey ratings</td>
</tr>
<tr>
<td></td>
<td>• Competitive costs</td>
<td>• Attainment of unit cost targets</td>
</tr>
<tr>
<td></td>
<td>• Development performance</td>
<td>• Major project scores</td>
</tr>
<tr>
<td></td>
<td>• Operational performance</td>
<td>• Attainment of targeted levels</td>
</tr>
<tr>
<td>Operational</td>
<td>• Development process</td>
<td>• Function point measures</td>
</tr>
<tr>
<td>excellence</td>
<td>• Operational process</td>
<td>• Change management effectiveness</td>
</tr>
<tr>
<td></td>
<td>• Process maturity</td>
<td>• Level of IT processes</td>
</tr>
<tr>
<td></td>
<td>• Enterprise architecture</td>
<td>• State of the infrastructure assessment</td>
</tr>
<tr>
<td>Future</td>
<td>• Human resource management</td>
<td>• Staff turnover</td>
</tr>
<tr>
<td></td>
<td>• Employee satisfaction</td>
<td>• Satisfaction survey scores</td>
</tr>
<tr>
<td></td>
<td>• Knowledge management</td>
<td>• Implementation of learned lessons</td>
</tr>
</tbody>
</table>
What are the questions?
To Uncover IT Issues...

- How often do IT projects fail to deliver what they promised?
- Are end users satisfied with the quality of the IT service?
- Are sufficient IT resources, infrastructure and competencies available to meet strategic objectives?
- What has been the average overrun of IT operational budgets? How often and how much do IT projects go over budget?
- How much of the IT effort goes to firefighting rather than enabling business improvements?
To Find Out How Management Addresses the IT Issues...

- How well are enterprise and IT objectives aligned?
- How is the value delivered by IT being measured?
- What strategic initiatives has executive management taken to manage IT’s criticality relative to maintenance and growth of the enterprise, and are they appropriate?
- Is there an up-to-date inventory of IT risks relevant to the enterprise? What has been done to address these risks?
IT Governance
Structures, Process & Relational Mechanisms
Peterson Model (2003) of IT Governance Structures, Process & Relationship Mechanisms
What are IT Governance Structural Mechanisms?

- IT organisation structure (including placement in the overall organization structure)
- Roles and responsibilities
- IT strategy committee
- IT steering committee
- CIO on Board
- project steering committees
- special advisory board
- special task force
What are IT Governance Process?

- Formal budgeting process
- Evaluation methods
- Balanced (IT) scorecards
- Strategic Information Systems Planning
- COBIT and ITIL
- Service Level Agreements
- Prioritization frameworks & information economics
- Strategic Alignment Model
- Business/IT alignment models
- IT Governance maturity models
Communications & Relationship Mechanisms

- Active participation by principle stakeholders
- Collaboration between principle stakeholders
- Partnership rewards and incentives (important!)
- Business/IT colocation

- Shared understanding of business/IT objectives
- Active conflict resolution (‘non-avoidance’)
- Cross-functional business/IT training
- Cross-functional business/IT job rotation
Holistic Approach

• Apakah mekanisme dari satu organisasi ke organisasi lainnya selalu sama?
• Suomi & Thahkakaa (2003) meneliti perbedaan rumah sakit pemerintah dan swasta.
• Hal yang membedakan antara lain:
  – Fleksibilitas dalam alokasi anggaran
  – Masalah fleksibilitas pengaturan SDM & organisasi
  – Masalah politik (di instansi publik)
  – Masalah kekakuan birokrasi dalam pengambilan keputusan
• Terlepas dari contoh di atas, selain berbeda dari satu organisasi ke organisasi lain, ternyata IT Governance tidak bisa statis! Bisa berubah tergantung kebutuhan dan tekanan eksternal (pasar, ekonomi, dsb.)
COBIT & IT Governance
COBIT
Control Objectives for Information and related Technology

- COBIT’s contains a framework responding to management’s need for control and measurability of IT by providing tools to *assess* and *measure* the enterprise’s IT capability for the 34 COBIT IT processes. The tools include:
  - Performance measurement elements (outcome measures and performance drivers for all IT processes)
  - A list of critical success factors that provides succinct, nontechnical best practices for each IT process
  - Maturity models to assist in benchmarking and decision-making for capability improvements
Framework IT Governance

Objectives

- IT is aligned with the business, enables the business and maximises benefits
- IT resources are used responsibly
- IT related risks are managed appropriately

IT Activities

- Planning and Organisation
- Acquisition and Implementation
- Delivery and Support
- Monitoring

<table>
<thead>
<tr>
<th>Manage risks</th>
<th>Realise Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>Increase Automation - be effective</td>
</tr>
<tr>
<td>reliability</td>
<td></td>
</tr>
<tr>
<td>compliance</td>
<td>Decrease Costs - be efficient</td>
</tr>
</tbody>
</table>
34 IT Process within COBIT 4.0
## IT Governance & COBIT Mappings

<table>
<thead>
<tr>
<th>Plan and Organise</th>
<th>Strategic Alignment</th>
<th>Value Delivery</th>
<th>Resource Management</th>
<th>Risk Management</th>
<th>Performance Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 Define a strategic IT plan.</td>
<td>H</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO2 Define the information architecture.</td>
<td>L</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>PO3 Determine technological direction.</td>
<td>M</td>
<td>S</td>
<td>S</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>PO4 Define the IT processes, organisation and relationships.</td>
<td>L</td>
<td>S</td>
<td>P</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>PO5 Manage the IT investment.</td>
<td>M</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>PO6 Communicate management aims and direction.</td>
<td>M</td>
<td>P</td>
<td></td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>PO7 Manage IT human resources.</td>
<td>L</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>PO8 Manage quality.</td>
<td>M</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>PO9 Assess and manage IT risks.</td>
<td>H</td>
<td>P</td>
<td></td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>PO10 Manage projects.</td>
<td>H</td>
<td>P</td>
<td>S</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acquire and Implement</th>
<th>Strategic Alignment</th>
<th>Value Delivery</th>
<th>Resource Management</th>
<th>Risk Management</th>
<th>Performance Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>A11 Identify automated solutions.</td>
<td>M</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>A12 Acquire and maintain application software.</td>
<td>M</td>
<td>P</td>
<td>P</td>
<td>S</td>
<td></td>
</tr>
<tr>
<td>A13 Acquire and maintain technology infrastructure.</td>
<td>L</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A14 Enable operation and use.</td>
<td>L</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
<tr>
<td>A15 Procure IT resources.</td>
<td>M</td>
<td>S</td>
<td>P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A16 Manage changes.</td>
<td>H</td>
<td>P</td>
<td>S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A17 Install and accredit solutions and changes.</td>
<td>M</td>
<td>S</td>
<td>P</td>
<td>S</td>
<td>S</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DS1 Define and manage service levels.</td>
<td>M</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>P</td>
</tr>
<tr>
<td>DS2 Manage third-party services.</td>
<td>M</td>
<td>P</td>
<td>S</td>
<td>P</td>
<td>S</td>
</tr>
</tbody>
</table>
• Dibuat oleh Central Computer & Telecommunications Agency (UK).
• Kalau COBIT menjelaskan apa yang harus dilakukan, maka IT menjelaskan bagaimana hal itu dilakukan.
Kerangka ITIL
Software Development Mgt
Implementation Management
Documentation Management
Application Management
Outsourcing Management
Security Management
Data & Backup Management
Disaster Recovery Mgt
Thank You