Information System Governance

Dr. Ir. Yeffry Handoko Putra, M.T

Bab 1 : Pendahuluan

UNIVERSITAS KOMPUTER INDONESIA

Buku Acuan

- [Weill] Weill, P. and Ross, J.W., (2004), IT Governance: how top performers manage IT decision rights for superior results, Harvard Business Scholl Press, Massachusetts
- [Grem] Van Grembergen, W., (2003), Strategies for Information Technology Governance, Idea Group Publishing, UK
- [Grem2] Van Grembergen, W., De Haes, S., (2009), Enterprise Governance of Information Technology : Achieving Strategy Alignment and value, Springer, New York
- [ITG] IT Governance Institute(2005), Governance of Extended Enterprise: Bridging Business and IT Strategeis, John Wiley and Sons, New Jersey
- [Ben] Bentley, W., Davis, P.T., (2010), Lean Six Sigma Secrets for CIO, CRC Press
- [Tar] Tarantino, A., (2008), Governance, Risk and Compliance Handbook, John Wiley and Sons, Inc.
- [ITG-Bench] IT Governance MetricMeasurement and benchmarking

Rencana Perkuliahan

1. IT Governance Framework
   - [Grem2] Chap 1 [ITG] Chap 5-6, [Weill] Chap 1, [Grem] Chap 1, [Tar] Chap 2
2. Allocating Decision Right
   - [Weill] Chap 3, 2
3. Mechanisms for Implementing IT Governance
   - [Weill] Chap 4
4. Strategy, Governance and Performance
   - [Grem2] Chap 3, [Weill] Chap 6, [Grem] Chap 2
5. Planning and Control
   - [ITG] Chap 5,6 , [Ben] Chap 2
6. Assesing Business-IT
   - [Ben] Chap 3
   - Balanced scorecard [Grem2] Chap IV, [Grem] Chap IV-VII
   - COBIT and Val IT [Grem2] Chap 5, [Grem] Chap XI
7. Benchmarking
   - {ITG-Bench] Chap 2]
8. Corporate Governance
   - [Tar] Chap 1

IS/IT Governance

- "IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategy and objectives" (ITGI, 2003).

- "IT governance is the organizational capacity exercised by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT" (Van Grembergen, 2002).

The five major drivers of IS governance are:

1. **The search for competitive advantage in the dynamically changing information economy through intellectual assets, information, and IT**
2. **Rapidly evolving governance requirements across the Organization for Economic Cooperation and Development (OECD), underpinned by capital market and regulatory convergence**
   - **Quality requirements — Quality, Cost, Delivery**
   - **Fiduciary requirements (COSO Report) — Effectiveness and Efficiency of operations;** Reliability of Information; Compliance with laws and regulations
   - **Security requirements — Confidentiality; Integrity; Availability**

The five major drivers of IS governance are:

1. **The search for competitive advantage in the dynamically changing information economy through intellectual assets, information, and IT**
2. **Rapidly evolving governance requirements across the Organization for Economic Cooperation and Development (OECD), underpinned by capital market and regulatory convergence**
3. **Increasing information- and privacy-related legislation (compliance)**
4. **The proliferation of threats to intellectual assets, information, and IT**
5. **The need to align technology projects with strategic organizational**

WHAT DOES IT GOVERNANCE COVER?

- **IT Strategic Alignment: "IT Alignment is a Journey, Not a Destination."**
- **IT Value Delivery: "IT Value is in the Eye of the Beholder."**
  - ← The basic principles of IT value are delivery on time, within budget and with the benefits that were promised

WHAT DOES IT GOVERNANCE COVER?

- **IT Strategic Alignment: "IT Alignment is a Journey, Not a Destination."**
- **IT Value Delivery: "IT Value is in the Eye of the Beholder."**

Competitive advantage, elapsed time for order/service fulfillment, customer satisfaction, customer wait time, employee productivity and profitability

WHAT DOES IT GOVERNANCE COVER?

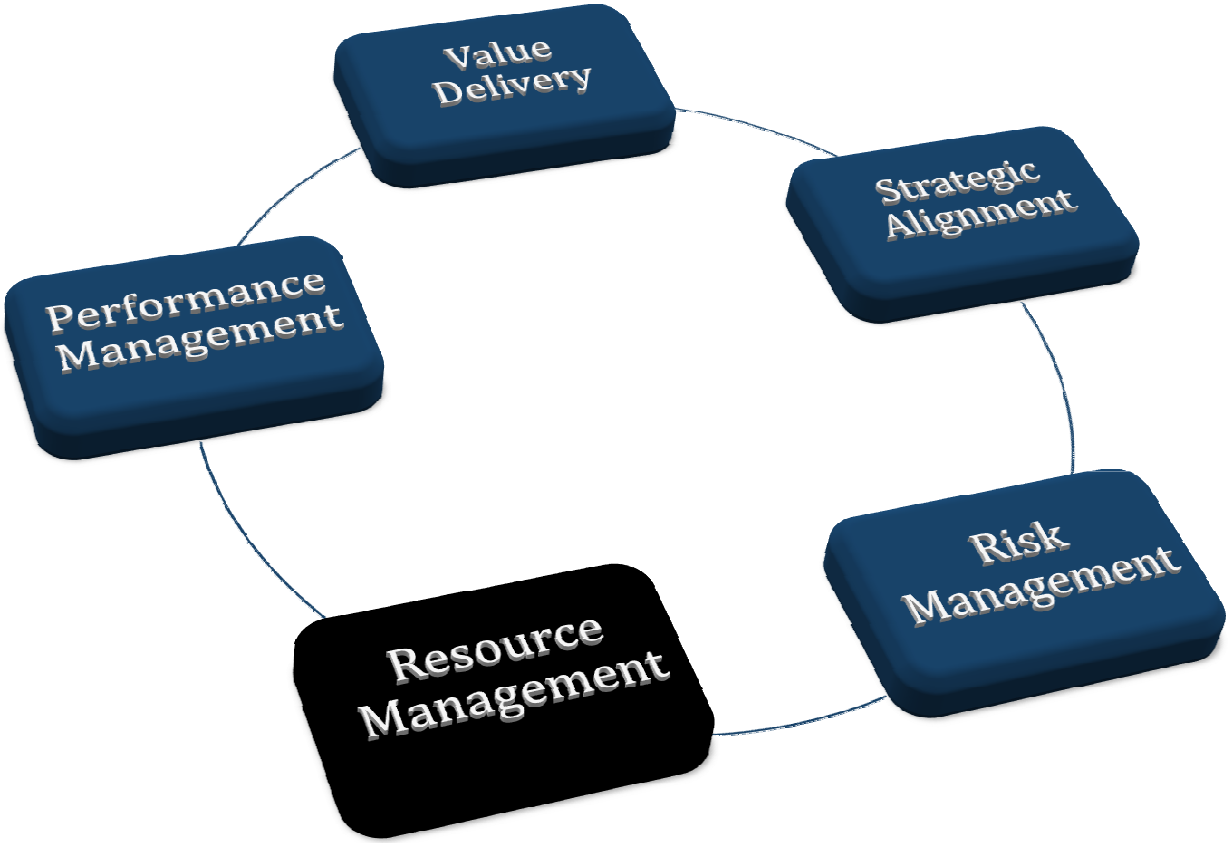
- **IT Strategic Alignment: "IT Alignment is a Journey, Not a Destination."**
- **IT Value Delivery: "IT Value is in the Eye of the Beholder."**
- **Performance Measurement: "In IT, if You're Playing the Game and Not Keeping Score, You're Just Practising."**
- **Risk Management: "It's the IT Alligators You Don't See that Will Get You."**

IT Governance Focus on

1. **Value delivery**
2. **Strategic alignment**
3. **Risk management**
4. **Resource management**
5. **Performance management**

maturity models, critical success factors (CSFs), key goal indicators (KGIs) and key performance indicators (KPIs)

IT Governance Focus on



Value Delivery, strategic alignment, risk management, Resource management, performance Management. (V, A, R, R, P)

IT Governance Guidance

- AS 8015-2005 (http://www.saiglobal.com/): Australian Standard for Corporate Governance of Information and Communication Technology.
- **CobiT** (Control Objectives for Information and Related Technology; http://itgi.org/): Another approach to standardize good IT control practices.
- **ISO/IEC 27001** (http://www.iso.org): A set of best practices for organizations to follow to implement and maintain a security program. It started out as British Standard 7799 (BS7799 Part 2). Typically organizations use ISO 27001 with another well-known ISO standard (ISO/IEC 27002, formerly ISO/IEC 17799).

IT Governance Guidance

- ISO/IEC 38500:2008 (http://www.iso.org): Another framework for effective governance of IT to assist those at the highest level of the organization to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organization's use of IT. ISO/IEC 38500 is applicable to organizations of all sizes, including public and private companies, government entities, and not-for-profit organizations. It provides guiding principles for directors of organizations on the effective, efficient, and acceptable use of IT within their organizations.
- Information Security Management Maturity Model (ISM3; http://www.ism3.com/): A process-based ISM maturity model for security.
- **IT Infrastructure Library** (ITIL; http://www.itil-officialsite.com/): A detailed framework with hands-on information on how to manage IT successfully.
- **Val IT** (http://www.itgi.org/): An enterprise value management framework for IT investments.

ISO principles for corporate governance of IT

Adapted from: ISO/IEC 38500:2008 – Corporate Governance of Information Technology

Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

Principle 2: Strategy

The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.

Principle 3: Acquisition

IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.

Principle 4: Performance

IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.

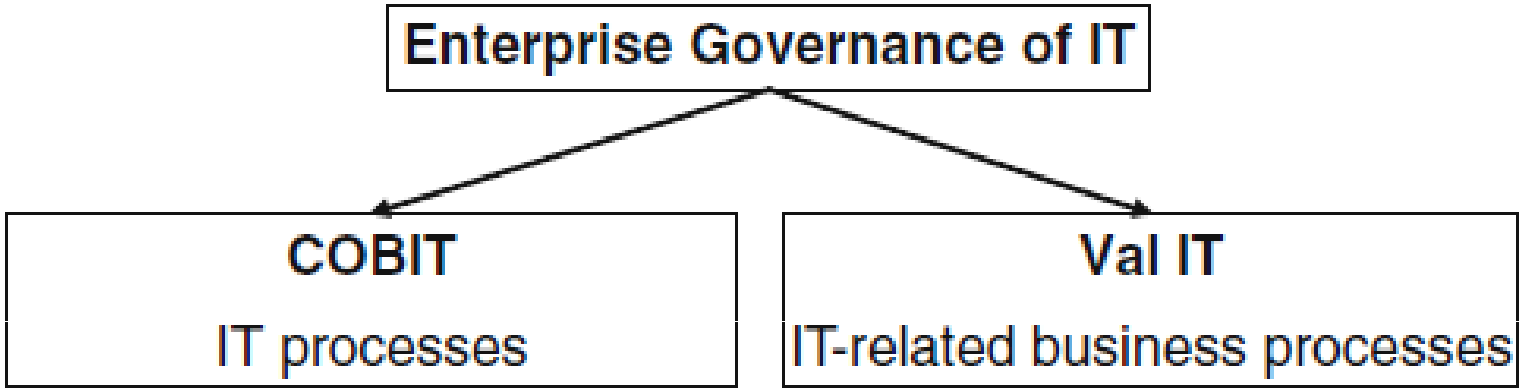
Principle 5: Conformance

IT complies with all mandatory legislations and regulations. Policies and practices are clearly defined, implemented and enforced.

Principle 6: Human Behavior

IT policies, practices and decisions demonstrate respect for Human Behavior, including the current and evolving needs of all the 'people in the process'.

Enterprise Governance of IT related to COBIT and Val IT



ISO 27000 Family of Standards

Standard	*Title*	*Description*
ISO 27000	Fundamentals and vocabulary	An overview and introduction to the ISO 27000 standards as a whole plus the specialist vocabulary used in ISO 27000.
ISO 27001 (Formerly BS 7799 Part 2)	Specification for an Information Security Management System	Information security management system requirements standard (specification) against which organizations are formally certified.
ISO 27002 (Formerly known as ISO 17799 and as BS 7799 Part 1)	Code of Practice for Information Security Management	Code of practice describing a comprehensive set of information security control objectives and a menu of best-practice security controls.
ISO 27003	Information Security Management System Implementation Guidance	Proposed implementation guide using PDCA.

ISO 27000 Family of Standards (2)

ISO 27004	Information Security Management—Measurement	Proposed information security management metrics and measurement standard to help measure the effectiveness of information security management system implementations.
ISO 27005	Information Security Risk Management	Proposed information security risk management standard (will replace the recently issued BS 7799 Part 3).
ISO 27006	Requirements for Bodies Providing Audit and Certification of Information Security Management Systems	A guide to the certification or registration process for accredited ISMS certification or registration bodies.
ISO 27007	Guidelines for Information Security Management Systems Auditing	A guideline for auditing information security management systems.

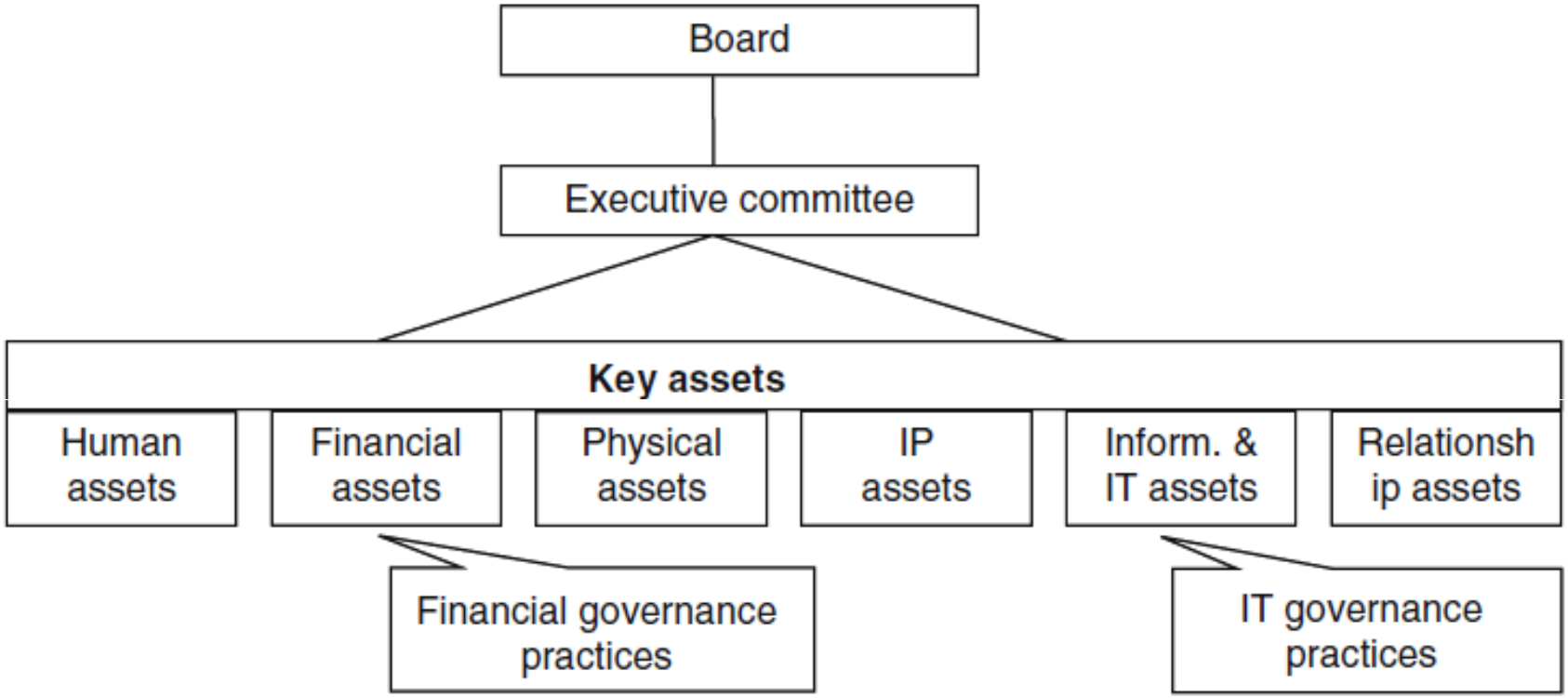
ISO 27000 Family of Standards (3)

Standard	*Title*	*Description*
ISO 27008	Guidance for Auditors on ISMS Controls (proposed title)	A guideline on auditing information security controls.
ISO 27010	Information Security Management Guidelines for Sector-to-Sector Interworking and Communications for Industry and Government (proposed title)	A guideline on sector-to-sector interworking and communications for industry and government, supporting a series of sector-specific ISMS implementation guidelines starting with ISO/IEC 27011.
ISO 27011	Information Security Management Guidelines for Telecommunications	A guideline for information security management for telecommunications (also known as X.1051)
ISO 27031	Specification for ICT Readiness for Business Continuity (proposed title)	ICT-focused standard on business continuity.

ISO 27000 Family of Standards (4)

ISO 27032	Guidelines for Cybersecurity	A guideline for cybersecurity.
ISO 27033	IT Network Security	Replace the multipart ISO/IEC 18028 standard on IT network security.
ISO 27034	Application Security	A guideline for application security.
ISO 2779	Health Informatics—information security management in health using ISO/IEC 27002	Additional information to assist healthcare professionals to implement ISO 27002.

6 Key asset to accomplish organization strategies and generate business value



Adapted from: Weill, P., and Ross, J., 2004, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Boston: Harvard Business School Press. Portions (CISR).

IP Asset=Intellectual Property