UNIVERSITAS KOMPUTER INDONESIA

Chap 3: COBIT

[Tar] Part 2

Dr. Ir. Yeffry Handoko Putra, M.T

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 (2)

- **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.

CobIT

Control Objectives for Information and Related Technology (CobiT)

- IT governance control framework.
- CobiT's purpose is to ensure IT resources are aligned with an enterprise's business objectives so that services delivered balance
- IT risks and returns.
- CobiT defines 34 significant processes, links 318 detailed controls activities to them, and defines an internal control framework for all of them.

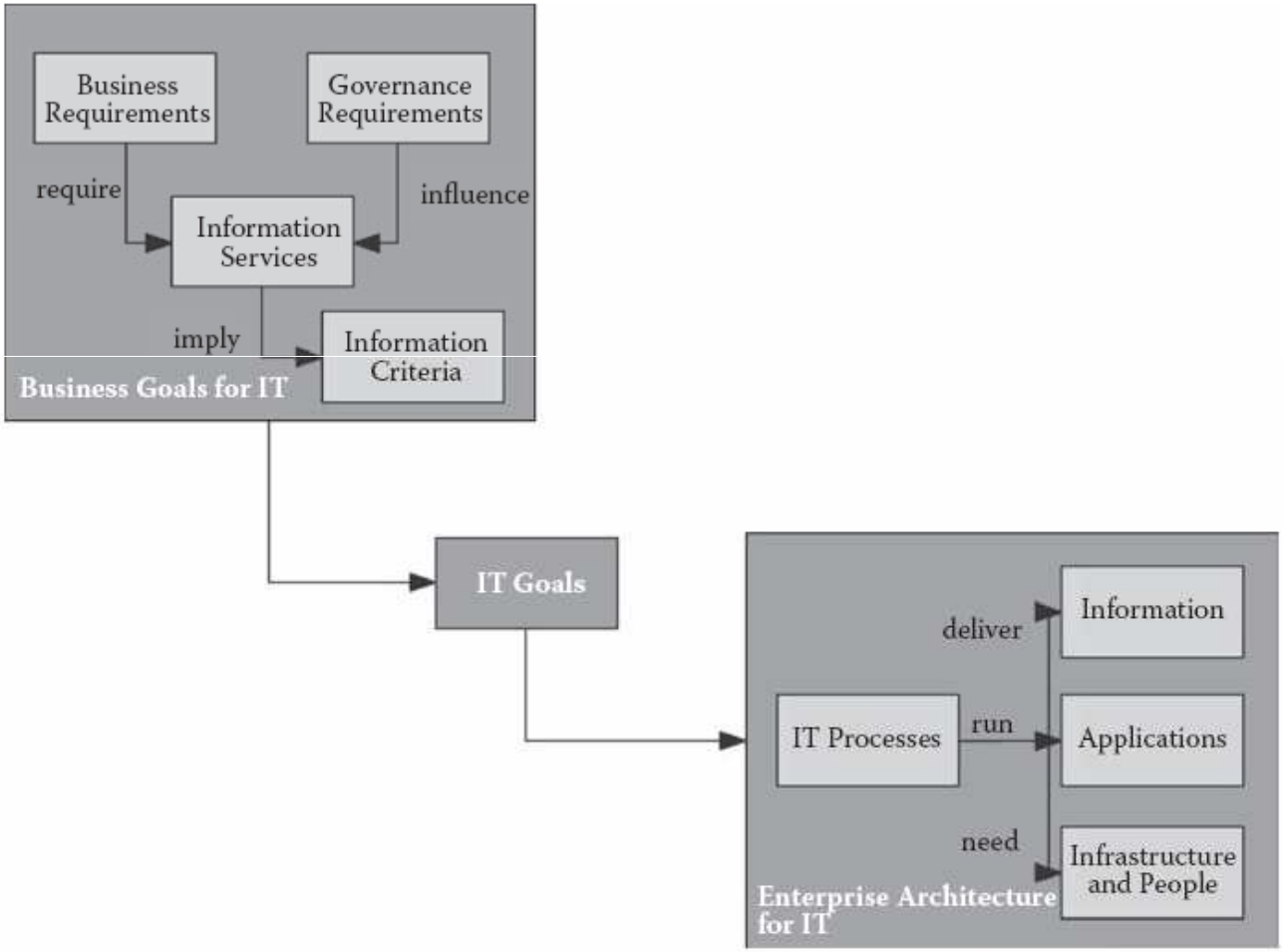
CobiT is designed for three distinct audiences

1. ***Management***—*to help them to balance risk and control investment in an* often unpredictable IT environment
2. ***Users***—*to obtain assurance on the security and controls of IT services*
3. ***Information systems auditors***—*to substantiate their opinions and/or to* provide better advice to management on internal controls

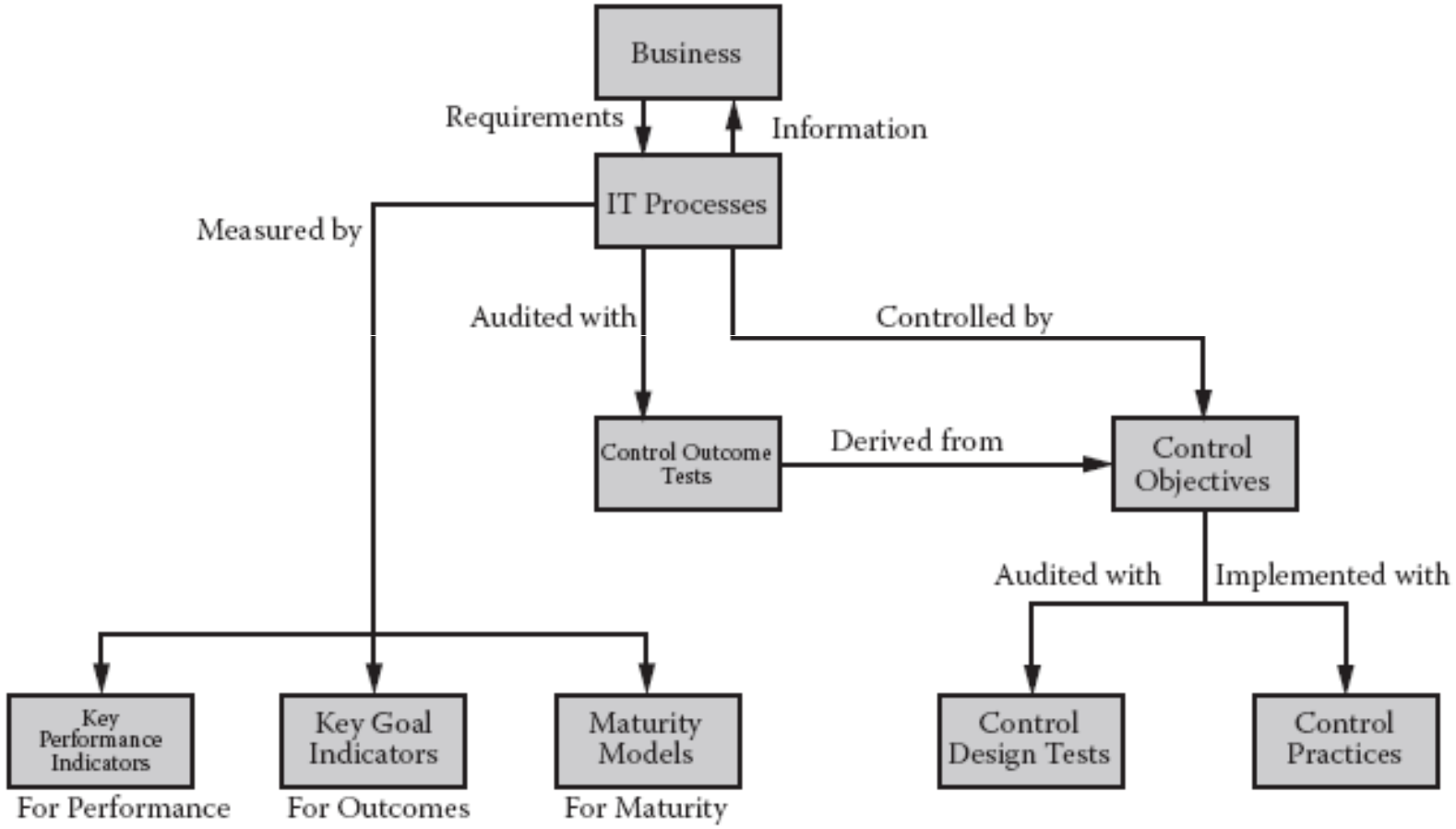
COBIT EVOLUTION SUMMARY

- 1994CobiT first edition—Audit
- 1998CobiT second edition—Control
- 2000CobiT third edition—Management
- 2005CobiT fourth edition—Governance

CobiT Framework



CobiT Flow


Business
Requirements
Information
IT Processes
Measured by
Audited with
Controlled by
Control Outcome Tests
Derived from
Control Objectives
Audited with
Implemented with
Key Performance Indicators
Key Goal Indicators
Maturity Models
Control Design Tests
Control Practices
For Performance
For Outcomes
For Maturity

CobiT's processes and control objectives are segmented into four domains

1. Planning and Organization (PO)
2. Acquisition and Implementation (AI)
3. Delivery and Support (DS)
4. Monitoring (M)

PLANNING AND ORGANIZATION

- Strategy and tactics for IT contribution
- Meeting business objectives
- Appropriately planned, communicated, and managed
- Proper organization and technological infrastructure
- PO1 Define a strategic IT plan
- PO2 Define the information architecture
- PO3 Determine the technological direction
- PO4 Define the IT organization and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and directions
- PO7 Manage human resources
- PO8 Ensure compliance with external requirements
- PO9 Assess risks
- PO10 Manage projects
- PO11 Manage quality

ACQUISITION AND IMPLEMENTATION

- Realization of IT strategy
- Solutions identified, developed or acquired, and implemented
- Solutions integrated into business process
- Change and maintenance of systems
- AI1 Identify automated solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology infrastructure
- AI4 Develop and maintain IT procedures
- AI5 Install and accredit systems
- AI6 Manage changes

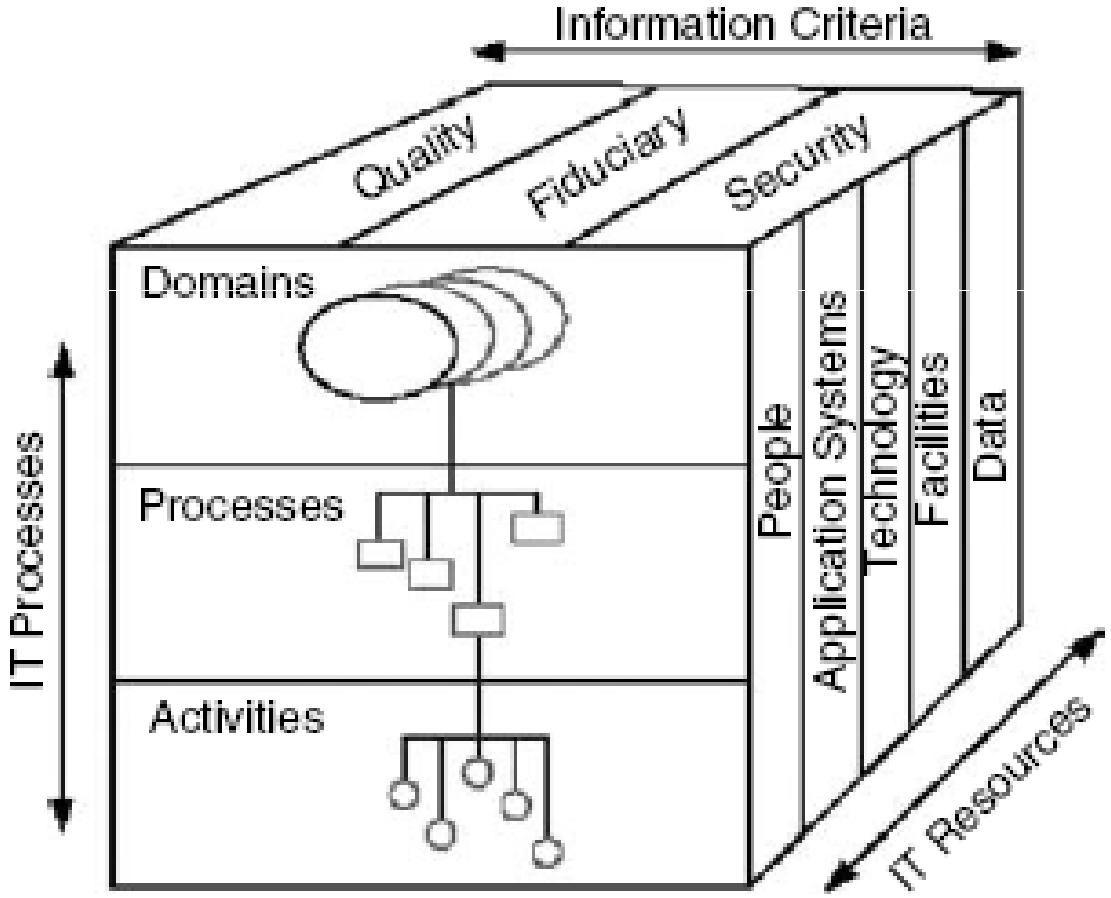
DELIVERY AND SUPPORT

- Actual delivery of required services
- Actual operations through security, including training
- Establishment of support processes
- Actual processing of data by applications
- DS1 Define and manage service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure system security
- DS6 Identify and allocate cost
- DS7 Educate and train users
- DS8 Assist and advise customers
- DS9 Manage the configuration
- DS10 Manage problems and incidents
- DS11 Manage data
- DS12 Manage facilities
- DS13 Manage operations

MONITORING

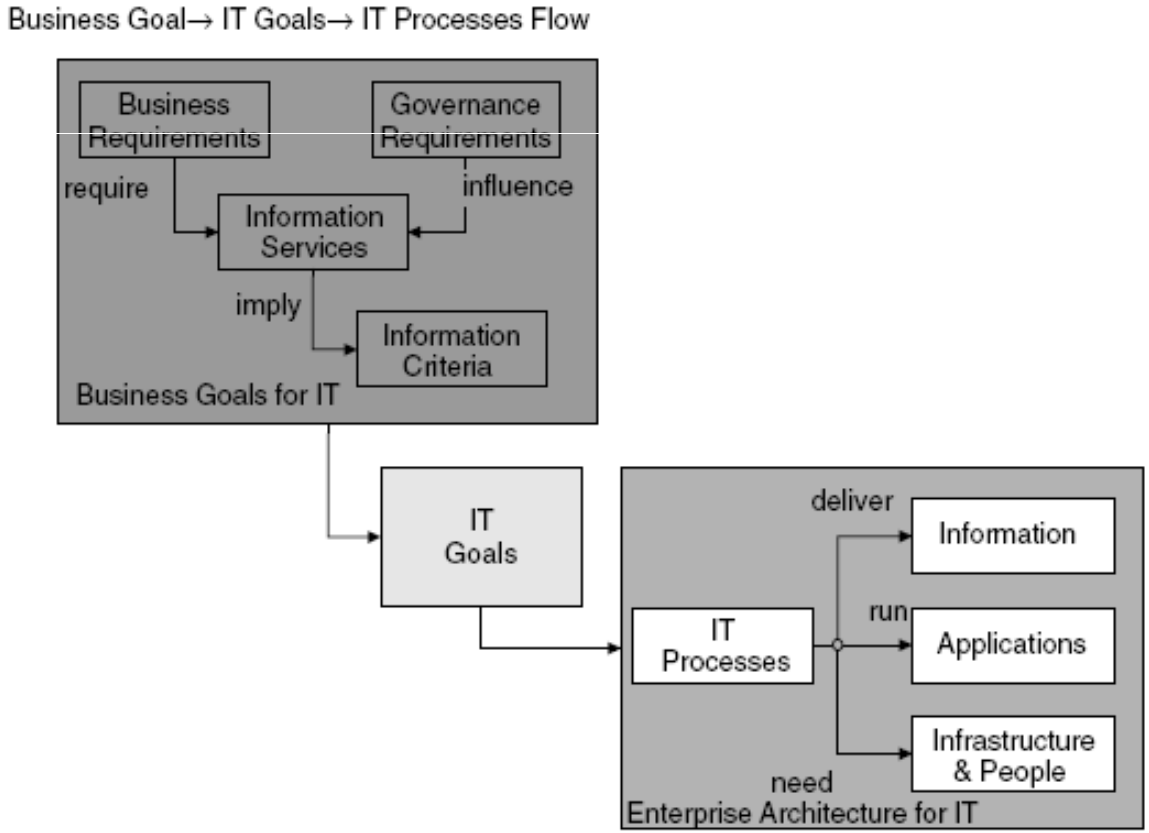
- Regular assessment of all IT processes
- Compliance with and quality of controls
- M1 Monitor the processes
- M2 Assess internal control adequacy
- M3 Obtain independent assurance
- M4 Provide for independent audit

CobIT Cube


Information Criteria
Quality
Fiduciary
Security
Domains
Processes
Activities
IT Processes
People
Application Systems
Technology
Facilities
Data
IT Resources

COBIT 4.x.

- CobiT 4.x offers an excellent linkage between business goals and IT goals/processes that was a missing component in the earlier version. Only four



Metrics link into the mapping of business goals to IT goals to IT processes

- *IT governance. CobiT 4.x contains a matrix mapping for all IT processes* to the governance domains.
- *Business requirements. Based on extensive research, a table is provided* showing the relationship among business goals, IT goals, and CobiT's IT processes to help users identify business-to-IT linkages in their own organizations.
- *Enterprise architecture. CobiT 4.x provides charts for identifying who* is responsible, accountable, consulted, and informed (RACI) to address process roles and responsibilities for each IT process.

COBIT 4.x MATURITY MODEL

1. Nonexistent..
2. Initial.
3. Repeatable.
4. Defined.
5. Managed.
6. Optimized.

LINKING BUSINESS GOALS TO IT GOALS

Business goals can be categorized at high level in four areas:

1. ***Financial perspective. Expand market share, increase revenue and return*** **on investment** (ROI), optimize asset utilization, and manage business risks.
2. ***Customer perspective. Improve customer service; offer competitive products*** and services, nonstop service availability, better time to market, and economical service delivery.
3. ***Internal perspective. Automate and integrate enterprise value chain,*** improve business process functionality, reduce process costs, comply with external laws and regulations, comply with internal policies, and improve operational productivity.
4. ***Growth perspective. Focus on business innovation, strategic decision making,*** and employee retention.

BUSINESS REQUIREMENTS MAPPING WITH IT RESOURCES/PROCESSES.

1. ***Quality***
   - *Effectiveness deals with information being relevant and pertinent to the* business process as well as being delivered in a timely, correct, consistent, and usable manner.
   - *Efficiency concerns the provision of information through the optimal (most* productive and economical) usage of resources
2. ***Security***
   - *Confidentiality concerns protection of sensitive information from unauthorized* disclosure.
   - *Integrity relates to the accuracy and completeness of information as well* as to its validity in accordance with the business's set of values and expectations.
   - *Availability relates to information being available when required by* the business process, and hence also concerns the safeguarding of resources.

BUSINESS REQUIREMENTS MAPPING WITH IT RESOURCES/PROCESSES.

3. *Fiduciary*

- *Compliance deals with complying with those laws, regulations, and contractual* arrangements to which the business process is subject (i.e., externally imposed business criteria).

- *Reliability of information relates to systems providing management with* appropriate information for it to use in operating the entity, in providing financial reporting to users of the financial information, and in providing information to report to regulatory bodies with regard to compliance with laws and regulations.