



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?

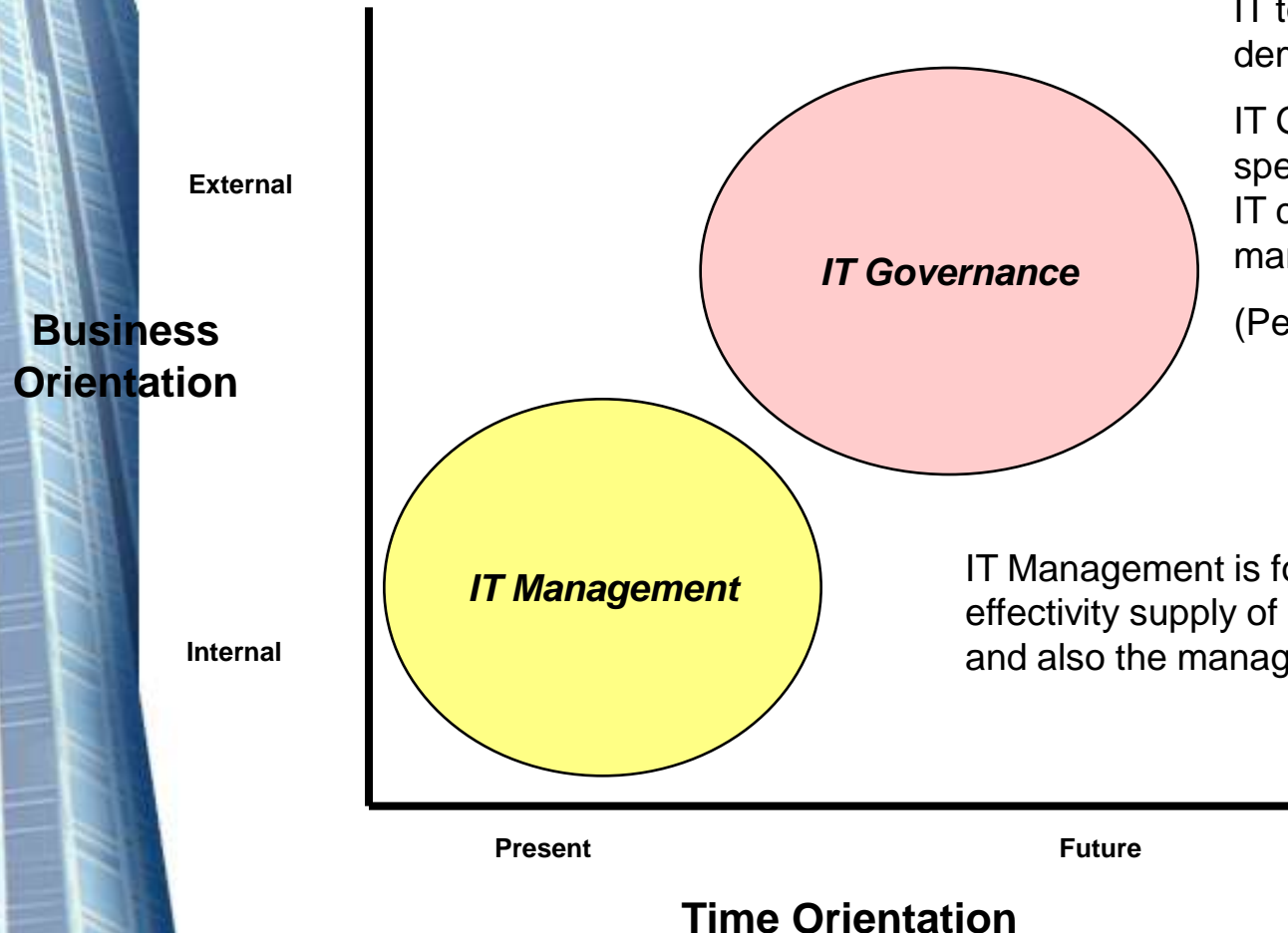
- IT governance is the responsibility of the board of directors (*komisaris*) and executive management.
- It is an integral part of enterprise governance and consists of the
 - leadership and
 - organisational structures and
 - processes
- that ensure that the organisation's IT sustains and extends the 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



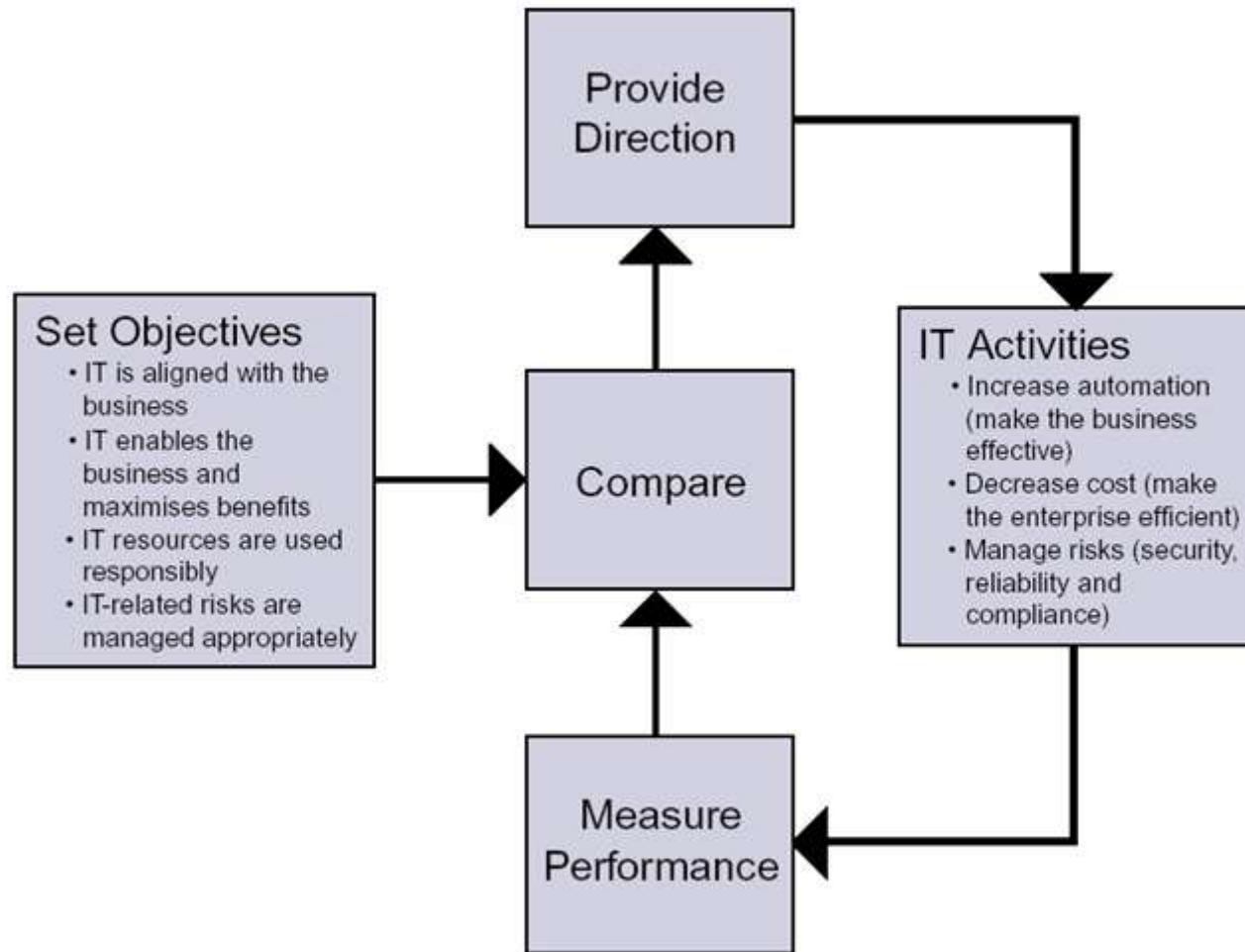
IT Governance concentrates on performing and transforming IT to meet present and future demands of business.

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

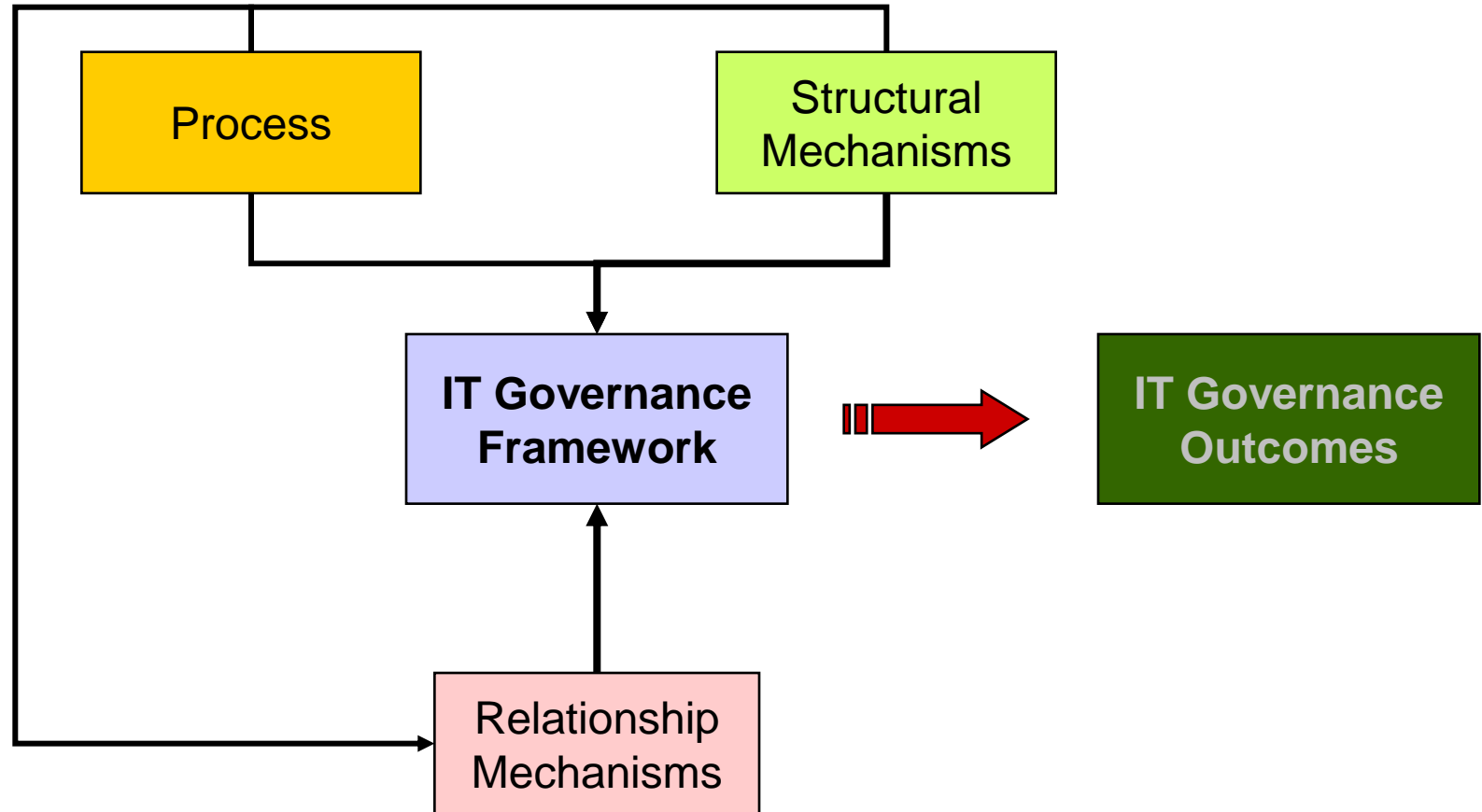
(Peterson, 2003)

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

IT Governance Framework



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.

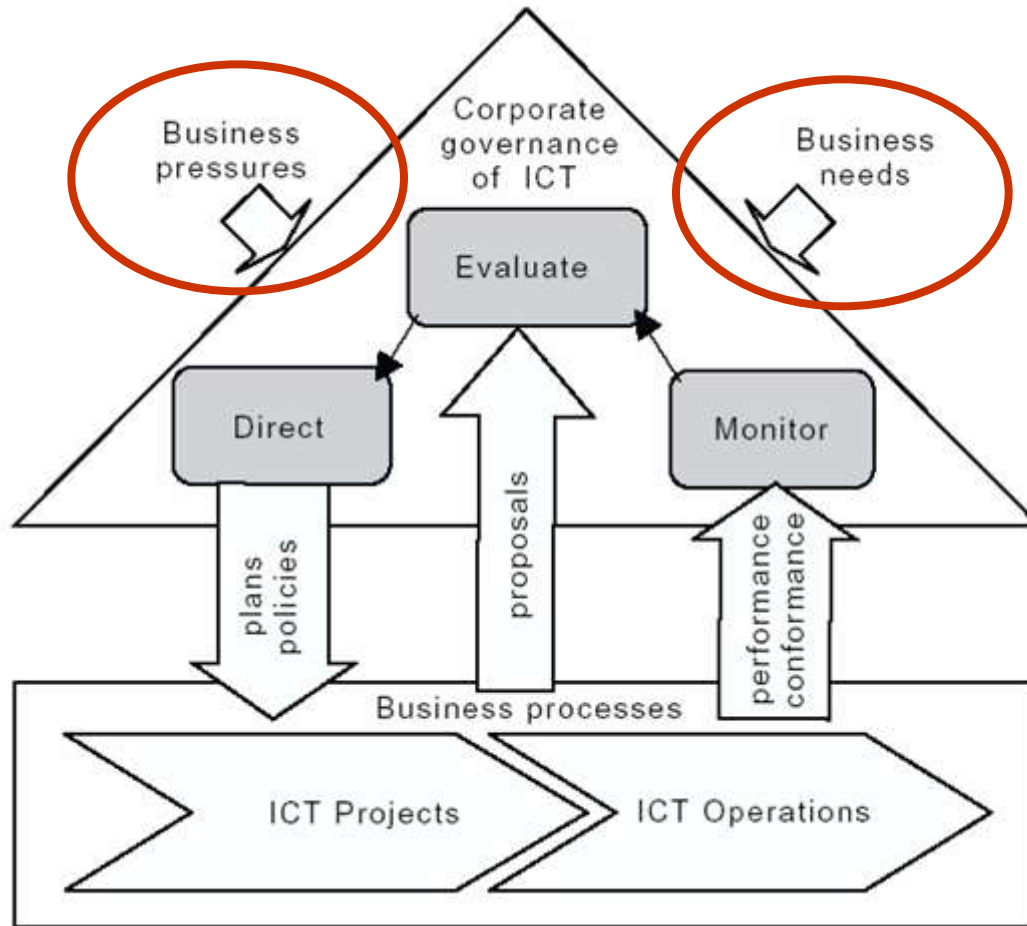


Why IT Governance?

- 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 depends 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 → introduce new opportunity or new risk!
7. Organization's GCG programme may require all areas to be governed properly.



IT Gov & GCG Questions

| Corporate Governance questions | ⇒ | IT Governance questions |
|--|---|---|
| How do suppliers of finance get managers to return some of the profits to them? | ⇒ | How does top management get their CIO and IT organisation to return some business value to them? |
| How do suppliers of finance make sure that managers do not steal the capital they supply or invest it in bad projects? | ⇒ | How does top management make sure that their CIO and IT organisations do not steal the capital they supply or invest in bad projects? |
| How do suppliers of finance control managers? | ⇒ | How does top management control their CIO and IT organisation? |

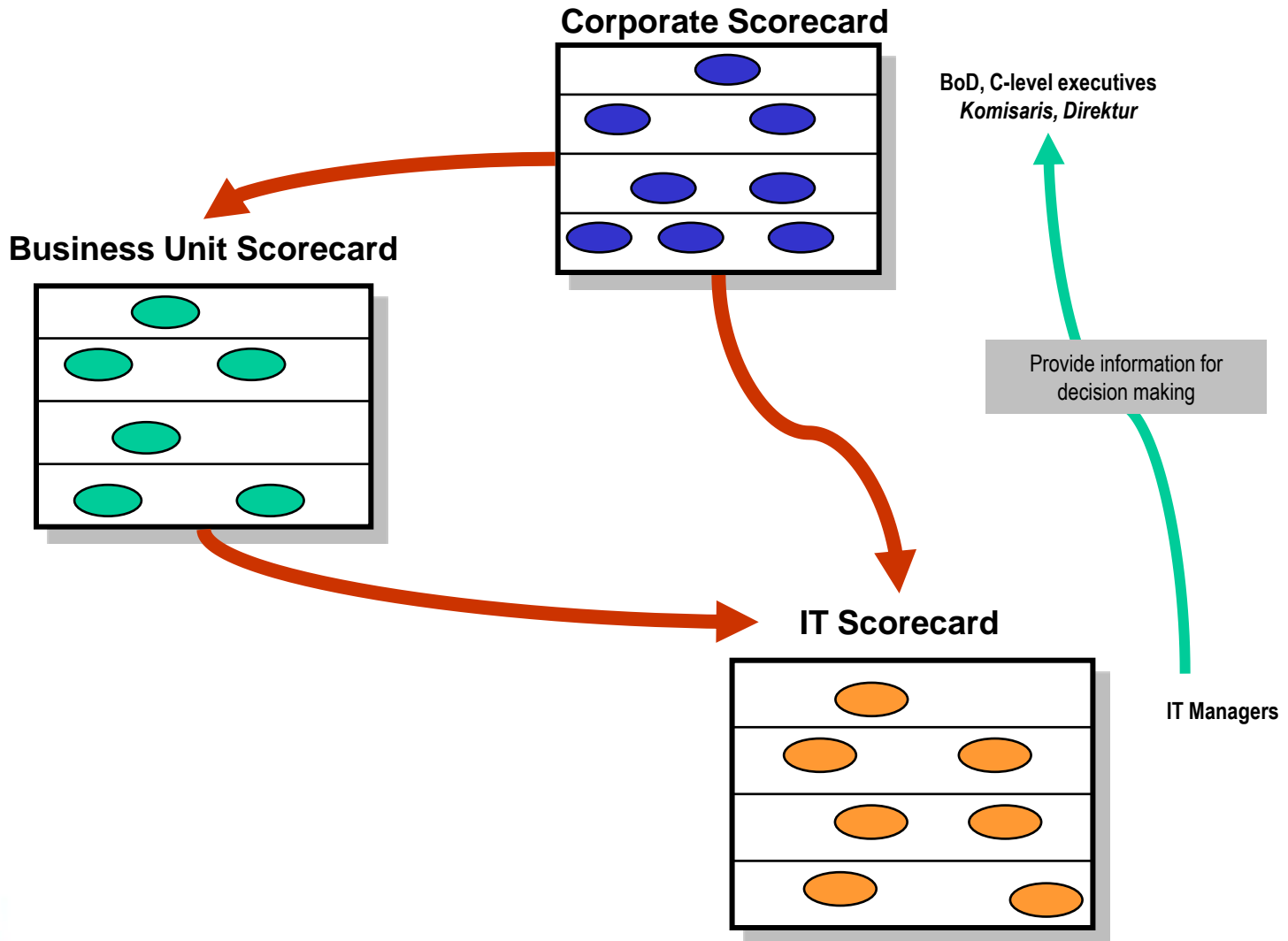
Whom does it concern?



All Levels...!

Cascaded objectives

BU Managers





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 amongst organizations).



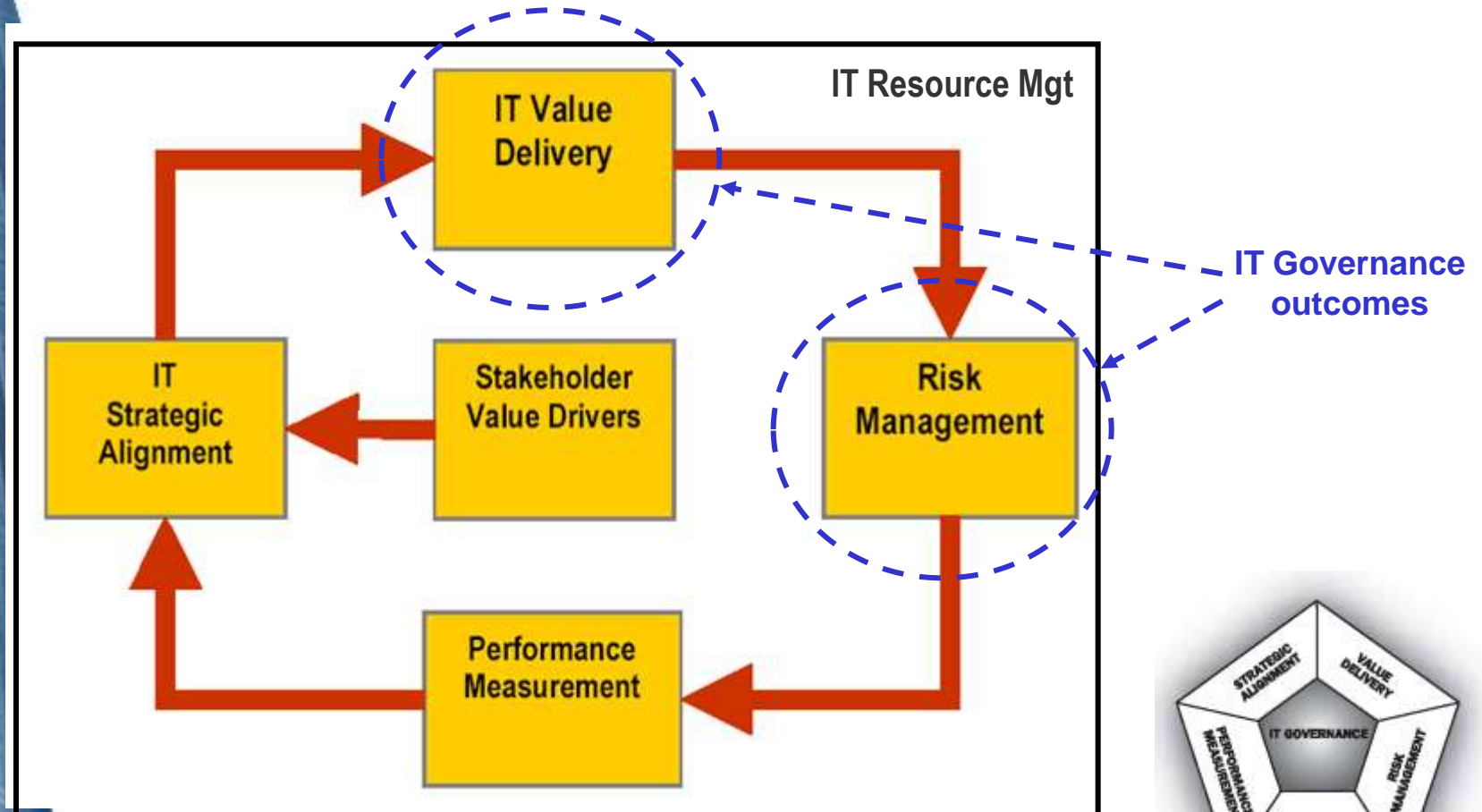
Senior Management / Top Executives

- 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 configured*)
 - *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

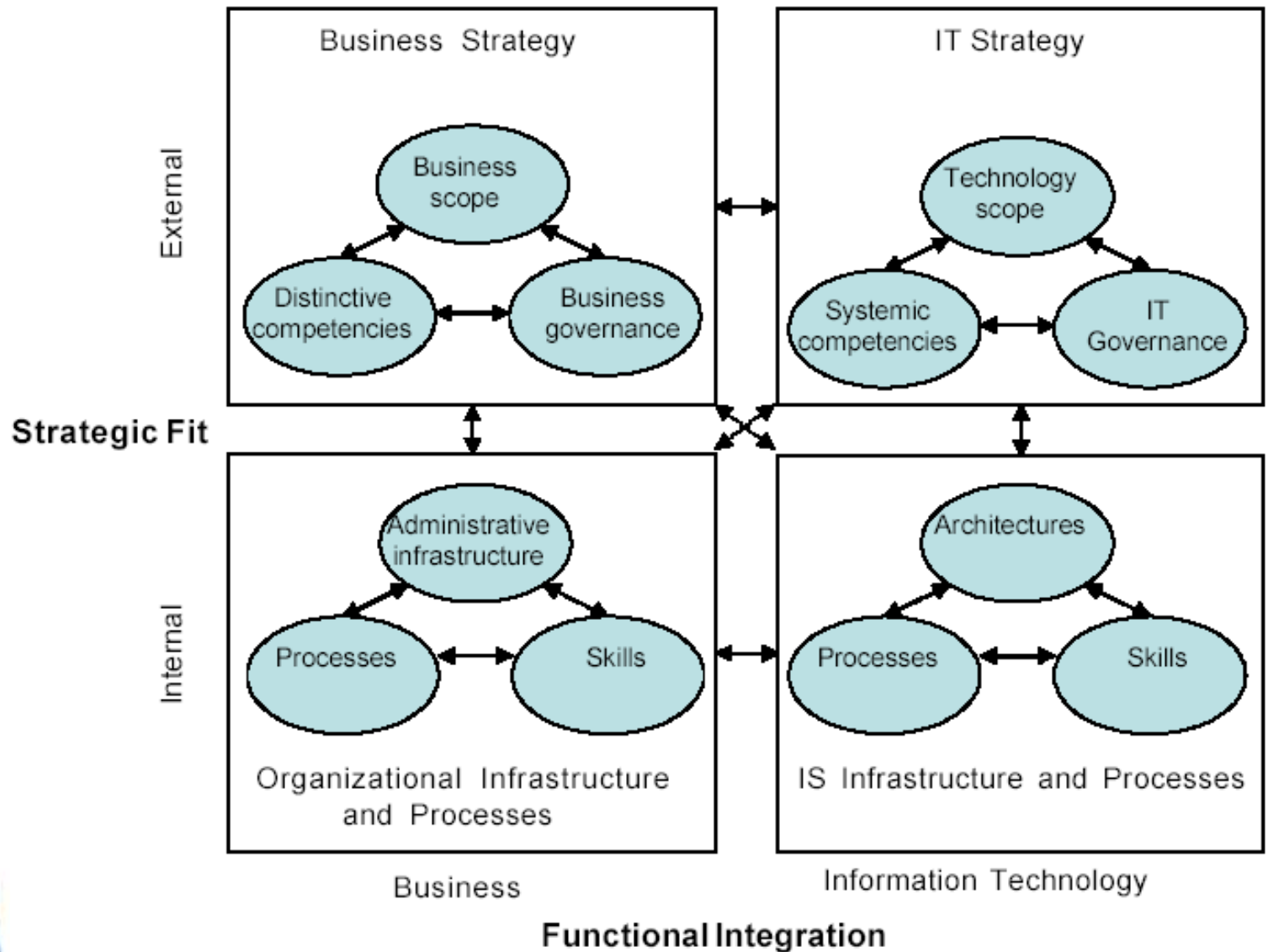
- IT Architecture
- IT Process (mis: system development maintenance)
- IT Skills, terkait masalah rekrutimen, pelatihan dan pengembangan SDM TI
- Problemnya, manager IT kebanyakan hanya memikirkan *internal domain decisions!*



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

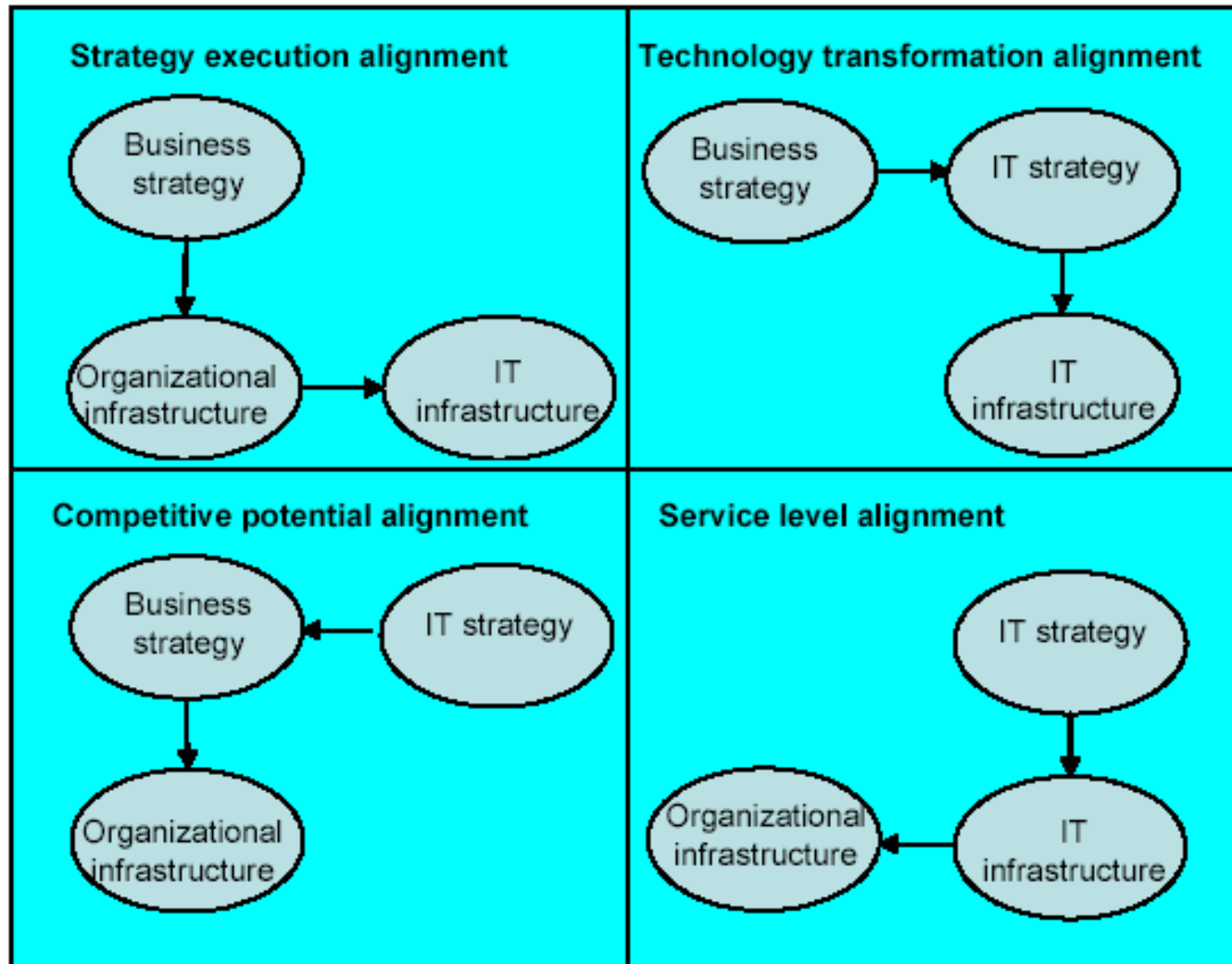




Strategic Alignment Domains

- 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





Strategic Alignment Types

- Strategic Execution:
 - Bersifat hirarkis 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/organisi 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

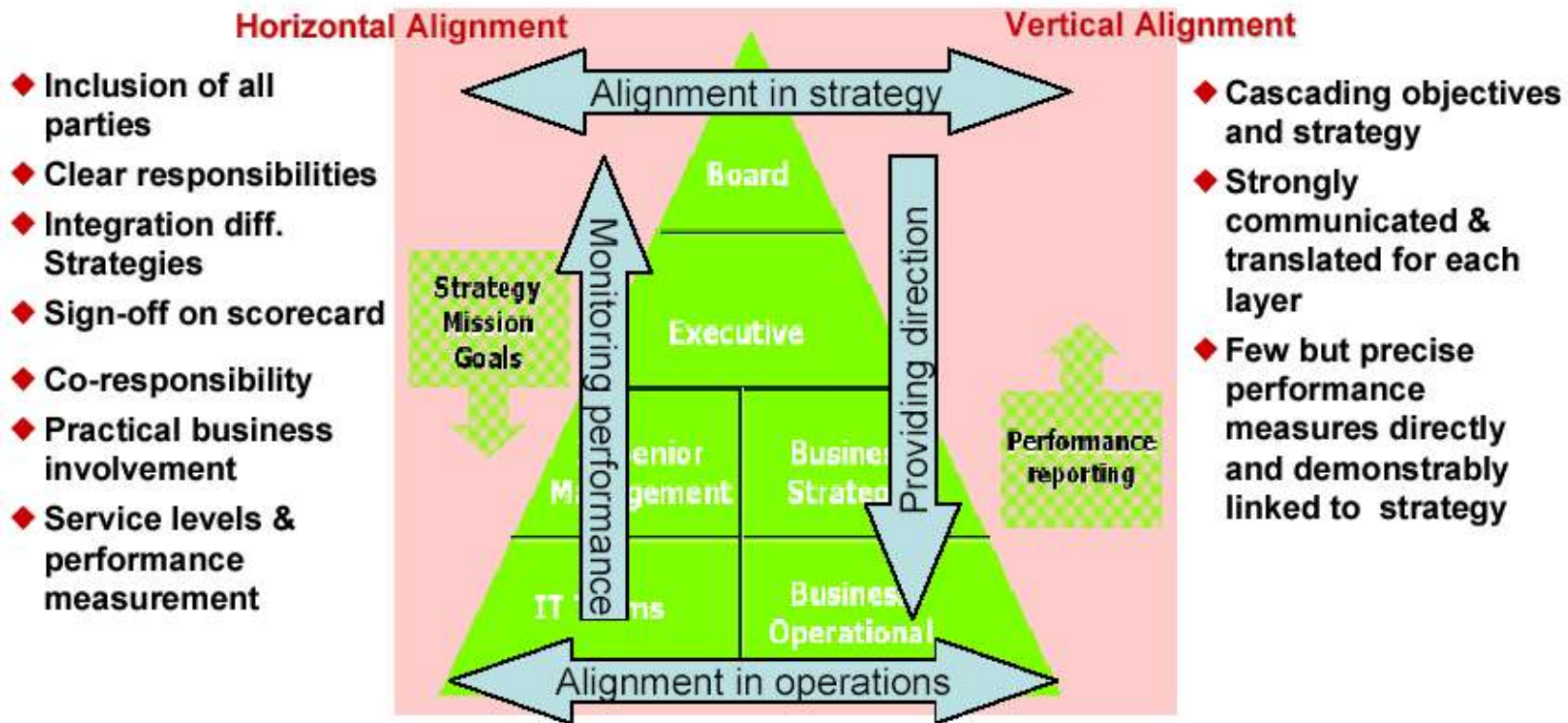
Specify the actions (project management)

Choose and evaluate success criteria

Sustain alignment

Vertical & Horizontal Alignment

Guldentops (2003)





Enablers & Inhibitors of Strategic Alignment

ENABLERS

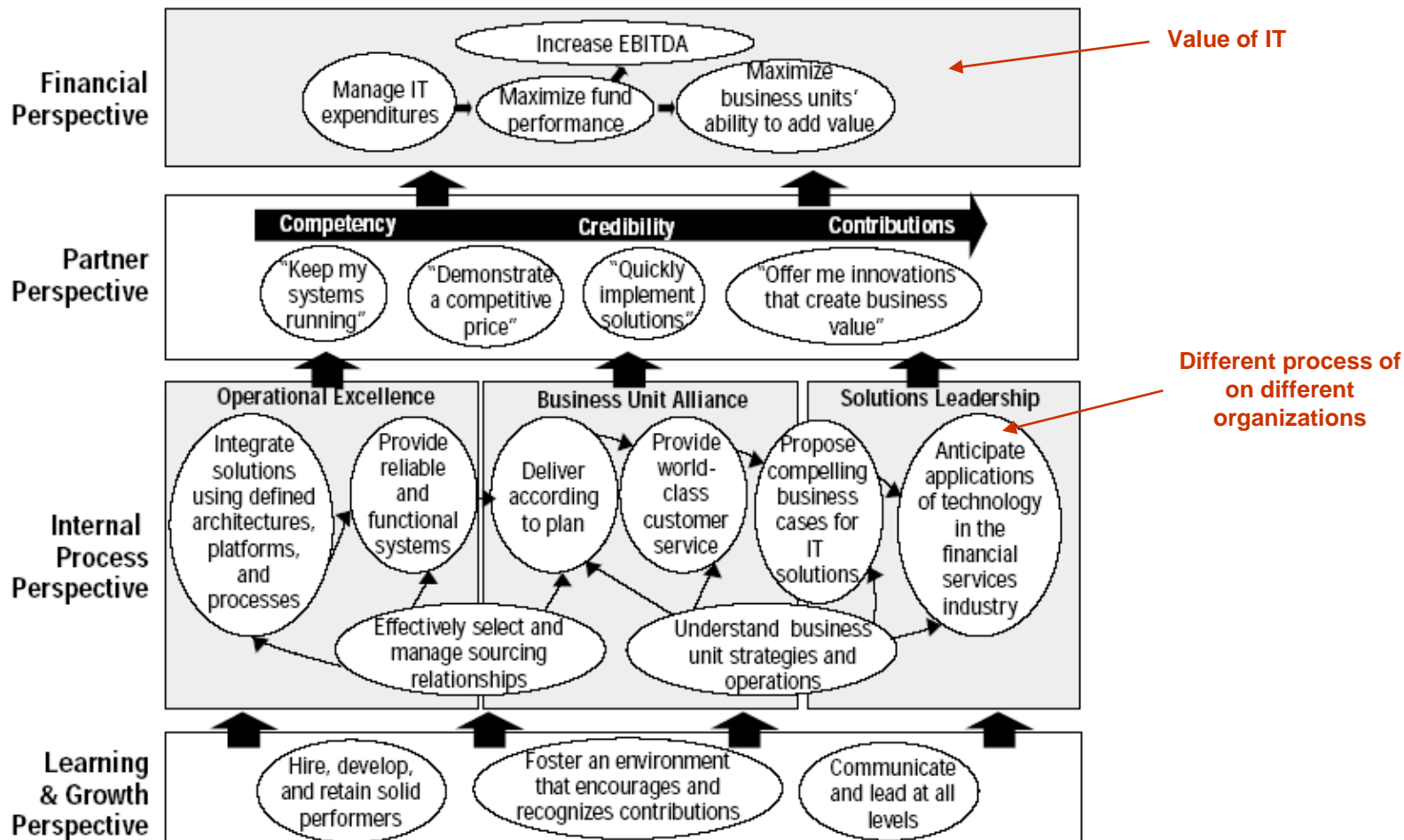
Senior executive support for IT
IT involved in strategy development
IT understands the business
Business-IT partnerships
Well-prioritised IT projects
IT demonstrates leadership

INHIBITORS

IT/business lack close relationships
IT does not prioritise well
IT fails to meet commitments
IT does not understand the business
Senior executives do not support IT
IT management lack leadership

IT Strategy drives IT Process

- Different strategy, different important process (e.g. mining vs banking)

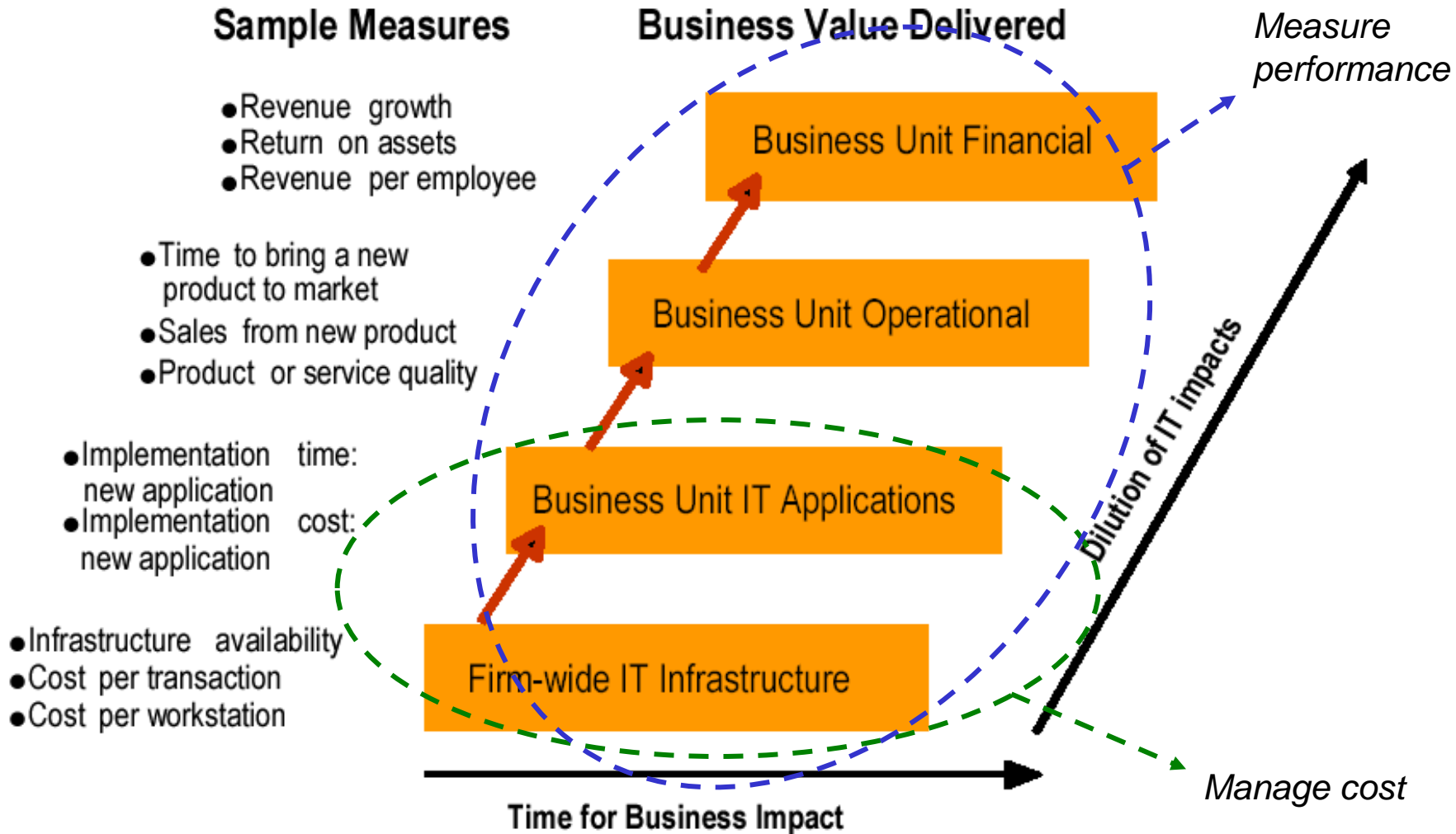




Value of IT at different levels of organization (Weill & Broadbent, 1998)

- 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)



Risk Management

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

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

Performance Measure

| Perspective | Objective | Example Metrics |
|------------------------|---|---|
| Corporate | <ul style="list-style-type: none">• Business/IT alignment• Value delivery• Cost management• Risk management• Intercompany synergy | <ul style="list-style-type: none">• Operational budget approval• Business unit performance• Attainment of expense and recovery targets• Results of internal audits• Single system solutions |
| Customer | <ul style="list-style-type: none">• Customer satisfaction• Competitive costs• Development performance• Operational performance | <ul style="list-style-type: none">• Business unit survey ratings• Attainment of unit cost targets• Major project scores• Attainment of targeted levels |
| Operational excellence | <ul style="list-style-type: none">• Development process• Operational process• Process maturity• Enterprise architecture | <ul style="list-style-type: none">• Function point measures• Change management effectiveness• Level of IT processes• State of the infrastructure assessment |
| Future | <ul style="list-style-type: none">• Human resource management• Employee satisfaction• Knowledge management | <ul style="list-style-type: none">• Staff turnover• Satisfaction survey scores• Implementation of learned lessons |

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?



Symptomatic

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?

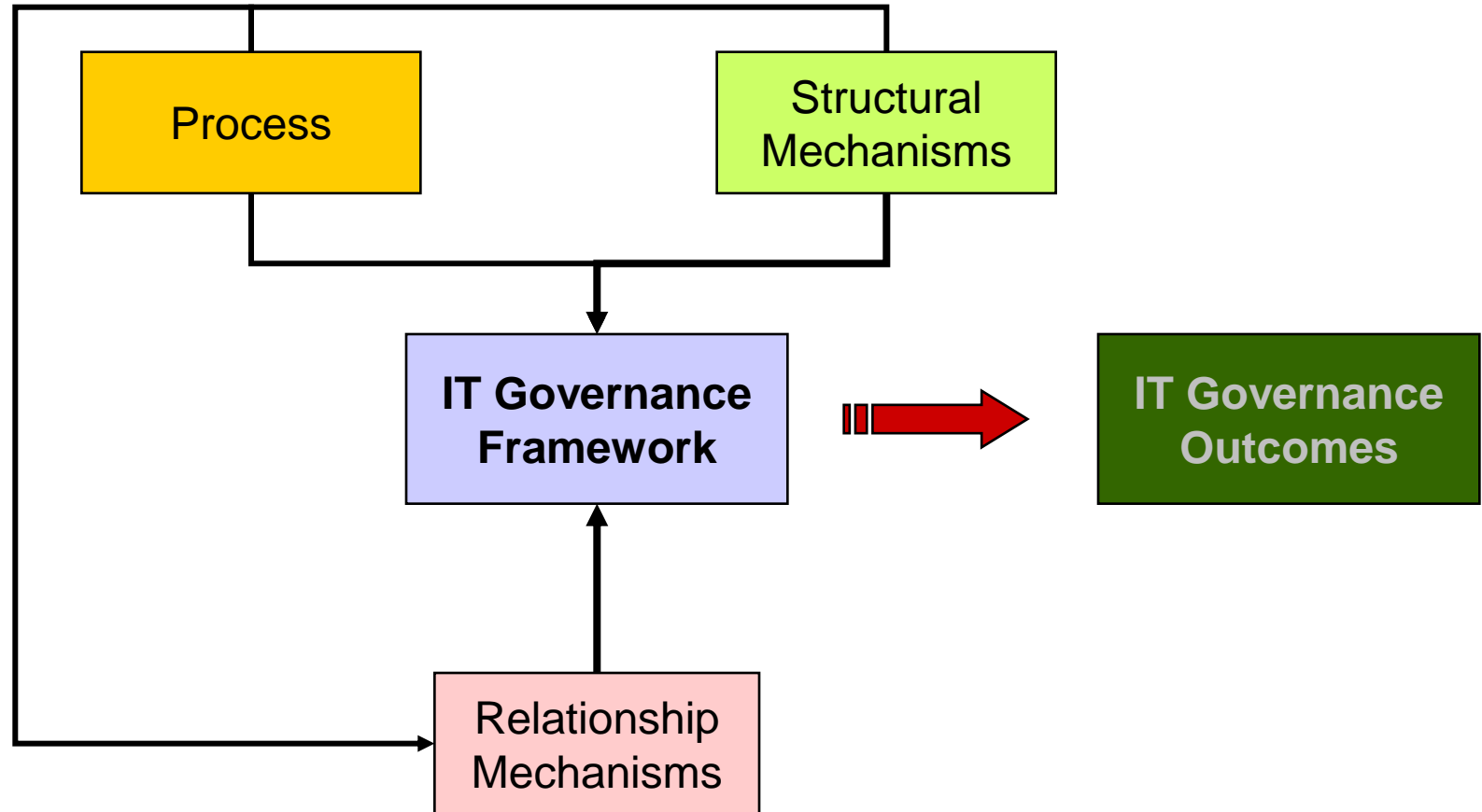



How do
they
manage!



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 & Thahkaka (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

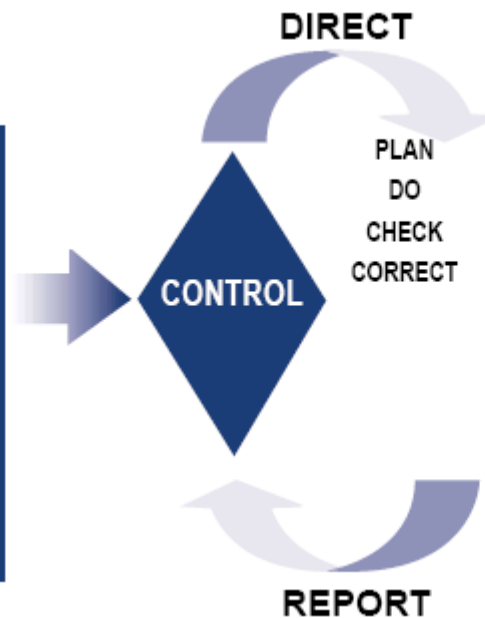
Control Objectives for Information and related Technology

- 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



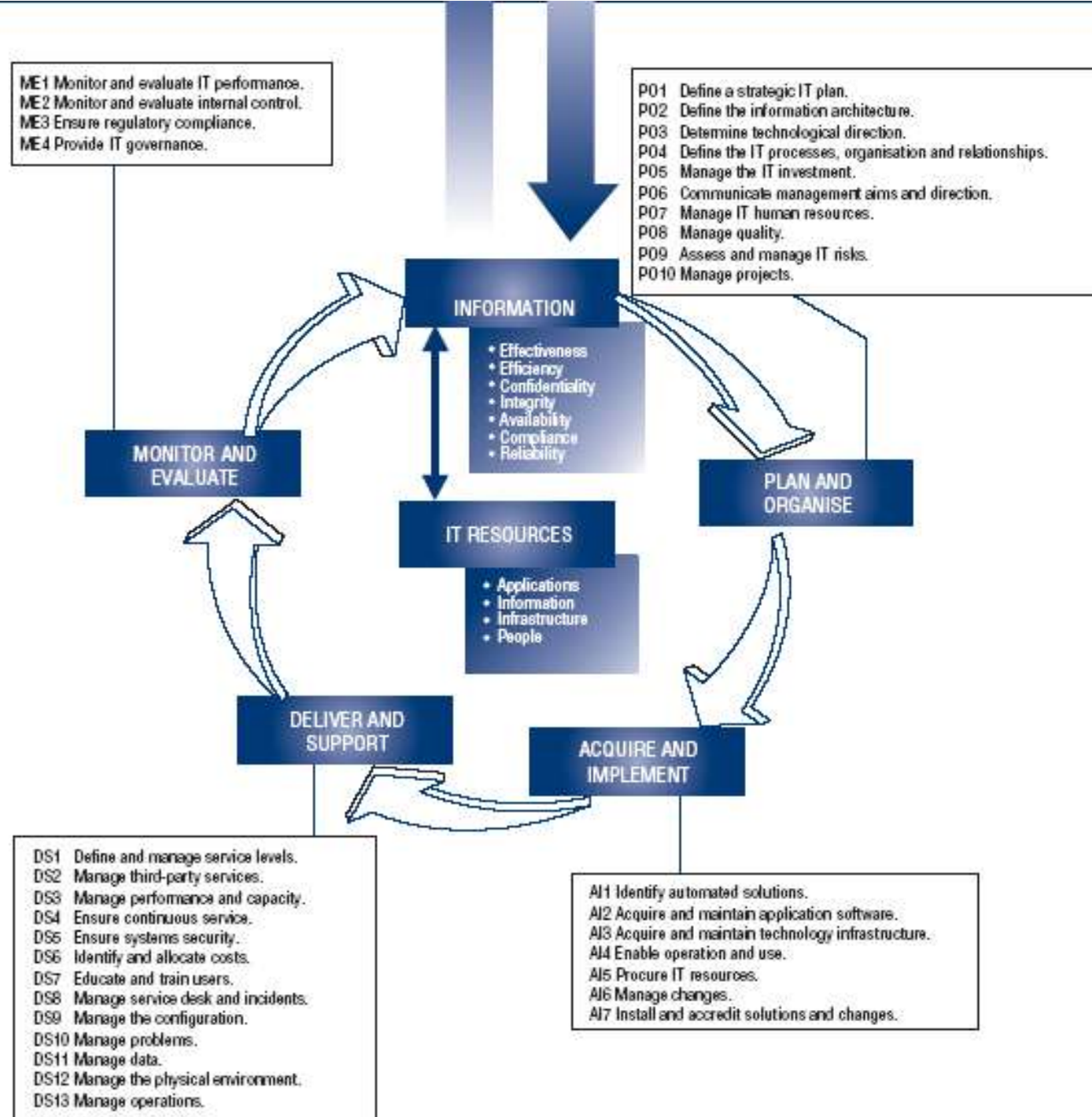
IT Activities

| | | |
|--|--|--|
| | | |
| | | |
| | | |
| | | |

Planning and Organisation
Acquisition and Implementation
Delivery and Support
Monitoring

| Manage risks | Realise Benefits | |
|---|--|-------------------------------------|
| <ul style="list-style-type: none">• security• reliability• compliance | Increase Automation - be effective | Decrease Costs - be efficient |

34 IT Process within COBIT 4.0



IT Governance & COBIT Mappings

IT Governance & IT Mappings

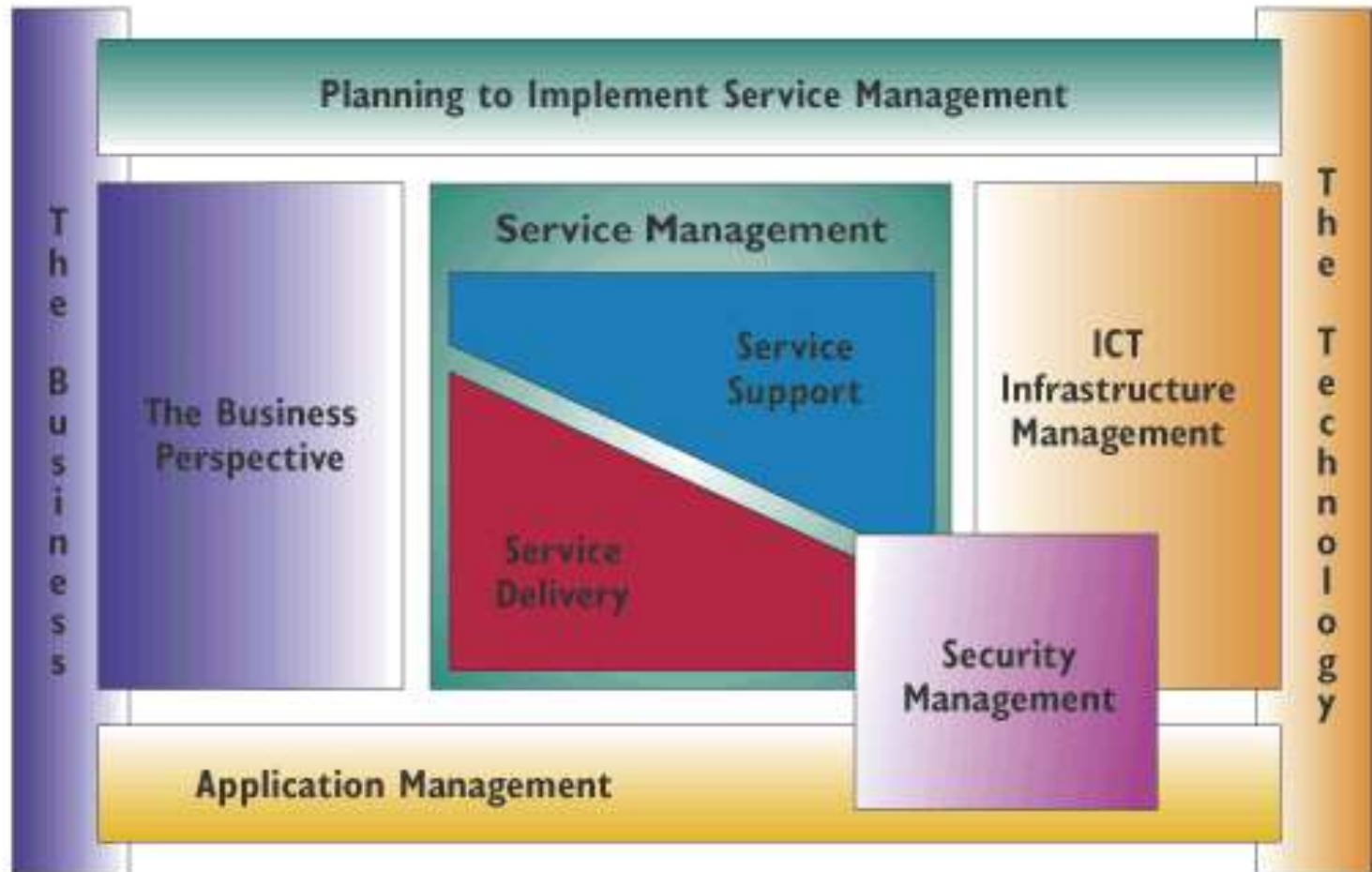
| | IMPORTANCE | IT Governance Focus Areas | | | | |
|--|------------|---------------------------|----------------|---------------------|-----------------|-------------------------|
| | | Strategic Alignment | Value Delivery | Resource Management | Risk Management | Performance Measurement |
| Plan and Organise | | | | | | |
| PO1 Define a strategic IT plan. | H | P | | S | S | |
| PO2 Define the information architecture. | L | P | S | P | S | |
| PO3 Determine technological direction. | M | S | S | P | S | |
| PO4 Define the IT processes, organisation and relationships. | L | S | | P | P | |
| PO5 Manage the IT investment. | M | S | P | S | | S |
| PO6 Communicate management aims and direction. | M | P | | | P | |
| PO7 Manage IT human resources. | L | P | | P | S | S |
| PO8 Manage quality. | M | P | S | | S | |
| PO9 Assess and manage IT risks. | H | P | | | P | |
| PO10 Manage projects. | H | P | S | S | S | S |
| Acquire and Implement | | | | | | |
| AI1 Identify automated solutions. | M | P | P | S | S | |
| AI2 Acquire and maintain application software. | M | P | P | | S | |
| AI3 Acquire and maintain technology infrastructure. | L | | | P | | |
| AI4 Enable operation and use. | L | S | P | S | S | |
| AI5 Procure IT resources. | M | | S | P | | |
| AI6 Manage changes. | H | | P | S | | |
| AI7 Install and accredit solutions and changes. | M | S | P | S | S | S |
| Deliver and Support | | | | | | |
| DS1 Define and manage service levels. | M | P | P | P | | P |
| DS2 Manage third-party services. | L | | P | S | P | S |

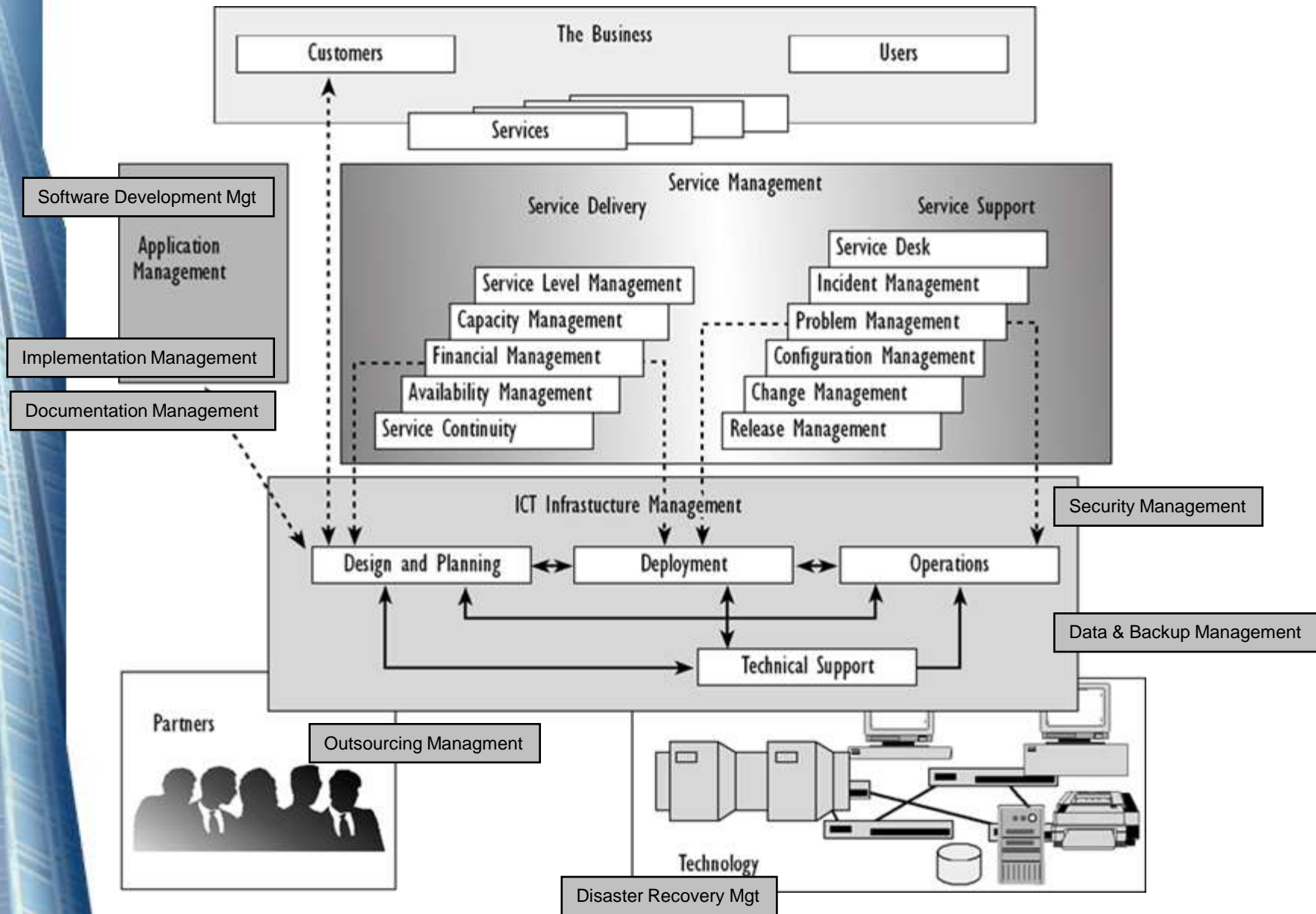


IT-IL

- Dibuat oleh Central Computer & Telecommunications Agency (UK).
- Kalau COBIT menjelaskan apa yang harus dilakukan, maka IT menjelaskan bagaimana hal itu dilakukan.

Kerangka ITIL





A low-angle photograph of a modern glass skyscraper reaching towards a bright sky. The building's facade is composed of numerous vertical glass panels, creating a grid-like pattern. In the foreground, a glass-walled structure, possibly a walkway or a lower part of the building, is visible, showing reflections of greenery. The sky is a pale, bright blue, and the overall lighting is soft and diffused.

Thank You