COBIT
Control Objectives for IT Related Technology

Arrianto Mukti Wibowo, M.Sc., CISA

IT Governance Lab
Faculty of Computer Science
University of Indonesia

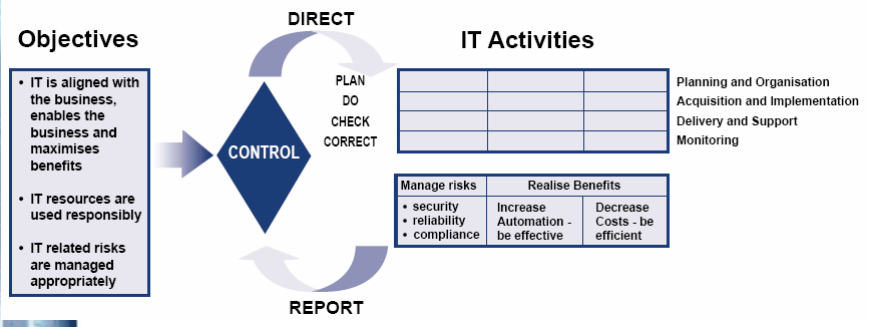
History

- Ditrigger oleh Committee of Sponsoring Organization (COSO) of Treadway Committee mengenai *Internal Controls – An Integrated Framework,* tahun 1980an yang *belum* memiliki panduan mengenai TI. Padahal laporan keuangan banyak dibuat oleh TI.
- Bermula dari EDP Auditor Association (sekarang bernama ISACA), cabang Eropa, yang membuat panduan control objectives.
- Dipelopori oleh Erik Guldentops, executive professor dari University of Antwerpen Management School, yang memulai inisiatif COBIT tahun 1994.
- Sekarang dikelola oleh COBIT Steering Committee dari IT Governance Institute (underbow ISACA)

Introduction

- Its mission is “to research, develop, publicize and promote an authoritative, up-to-date, international set of *generally accepted information technology control objectives* for day-to-day use by business managers and auditors.”
- Managers, auditors, and users benefit from the development of COBIT because it helps them understand their IT systems and decide the level of security and control that is necessary to protect their companies’ assets through the development of an IT governance model.
  - Business managers: IT dashboard
  - IT management: to communicate performance or to direct subordinates
  - IT staff: to build capability to perform daily duty to meet business expecations.

Framework IT Governance

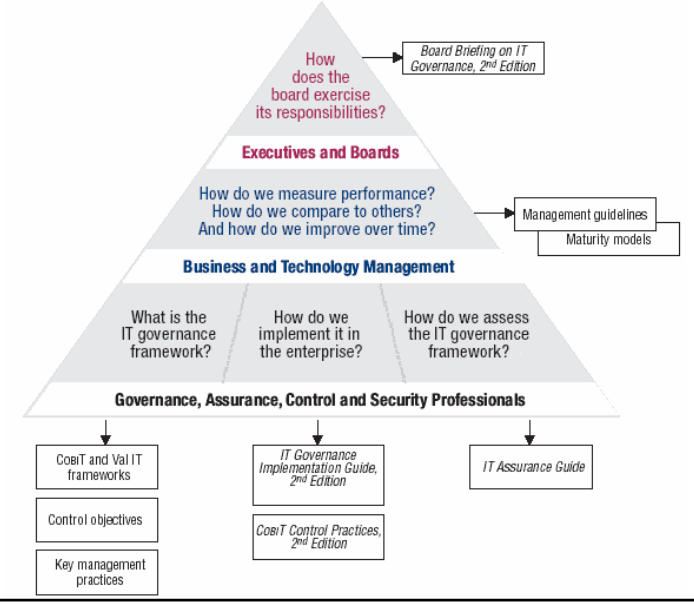


COBIT focuses primarily on what is required rather than how to undertake the activities themselves.

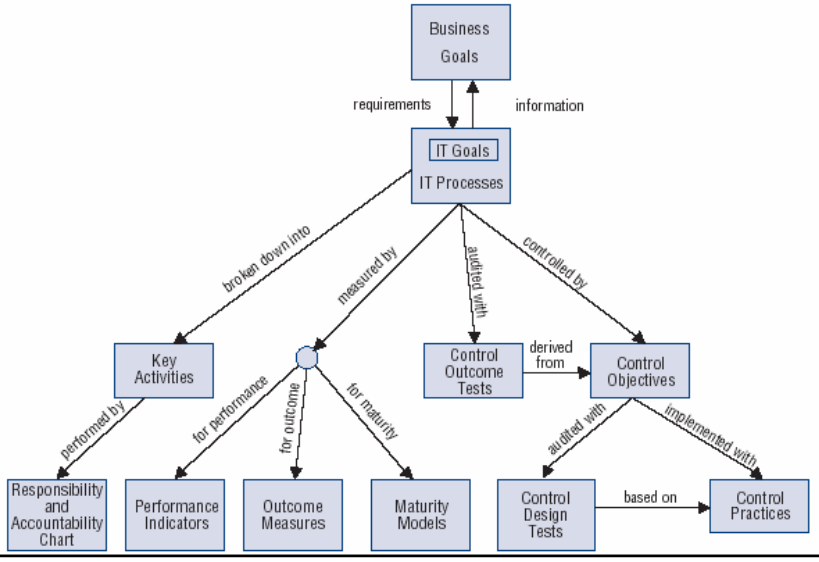
Sifat COBIT

- Lebih condong pada “business requirements for IT”
- Tidak memfokuskan diri pada praktek-praktek teknis
- Oleh karena itu, sangat menarik bagi orang-orang bisnis yang non-teknis.
- Tapi kurang menarik bagi orang teknis yang perlunya detailed day by day ‘how-to’.

COBIT content diagram



Interrelaitonship of COBIT Components



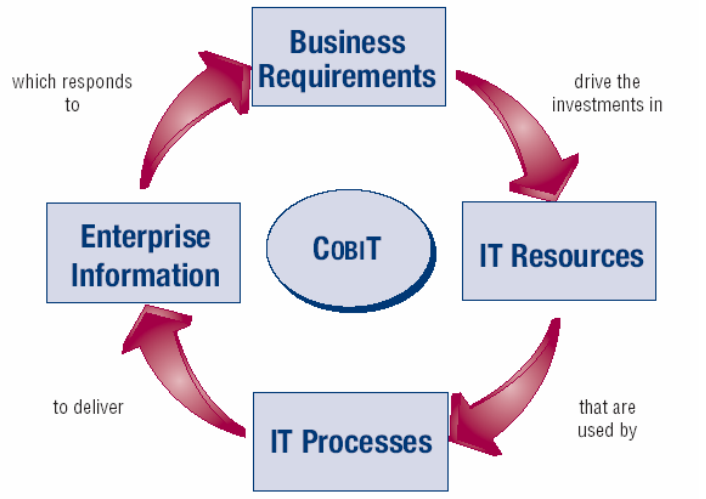
Pendekatan Dari COBIT

By being:

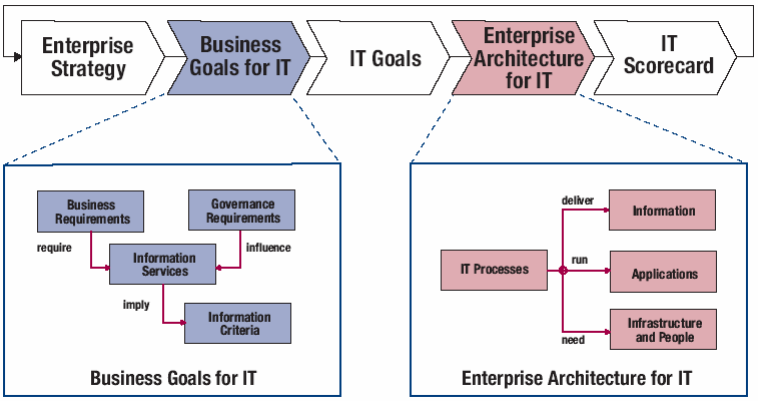
- Business Focused
- Process Oriented
- Control Based
- Measurement Driven

COBIT as a business focused tool

Basic COBIT principles



Defining IT Goals and Enterprise Architecture for IT



(baca penjelasan pada slide berikut)

Defining IT Goals and Enterprise Architecture for IT

- If IT is to successfully deliver services to support the enterprise's strategy, there should be:
  - a clear ownership and direction of the requirements by the business (the customer) and
  - a clear understanding of what needs to be delivered, and
  - how to do it, by IT (the provider).
- **Previous slide** illustrates how the enterprise strategy should be translated by the business into objectives related to IT-enabled initiatives (the business goals for IT).
- These objectives should lead to:
  - a clear definition of IT's own objectives (the IT goals),
  - which in turn define the IT resources and capabilities (the enterprise architecture for IT) required to successfully execute IT's part of the enterprise's strategy.

Linking Business Goal to IT Goal Pada Appendix I, COBIT 4.1

LINKING BUSINESS GOALS TO IT GOALS

		Business Goals	IT Goals							CobiT Information Criteria						
										Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24													
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22							
	3	Improve corporate governance and transparency.	2	18													
Customer Perspective	4	Improve customer orientation and service.	3	23													
	5	Offer competitive products and services.	5	24													

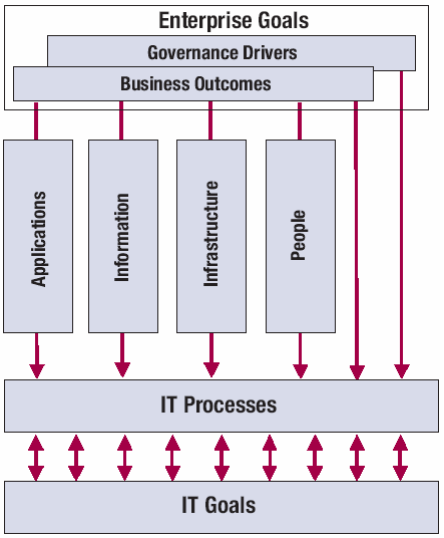
LINKING IT GOALS TO IT PROCESSES

	IT Goals	Processes										CobiT Information Criteria						
												Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	P	P		S	S		
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4						P	P					
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimise the use of information.	PO2	DS11										S		P			S
5	Create IT agility.	PO2	PO4	PO7	AI3							P	P		S			
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6								P	P				S	
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5								P	P				S	
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5									S	P					
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5									P	P					
10	Ensure mutual satisfaction of third-party relationships.	DS2										P	P	S	S	S	S	S
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7								P	P		S	S		
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				P	P				S	S
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8						P	S					

IT PROCESS TO IT GOALS MATRIX

	1 Respond to business requirements in alignment with the business strategy.	2 Respond to governance requirements in line with board direction.	3 Ensure satisfaction of end users with service offerings and service levels.	4 Optimise use of information.	5 Create IT agility.	6 Define how business functional and control requirements are translated in effective and efficient automated solutions.	7 Acquire and maintain integrated and standardised application systems.	8 Acquire and maintain an integrated and standardised IT infrastructure.	9 Acquire and maintain IT skills that respond to the IT strategy.	10 Ensure mutual satisfaction of third-party relationships.	11 Ensure seamless integration of applications into business processes.	12 Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	13 Ensure proper use and performance of the applications and the technology solutions.	14 Account for and protect all IT assets.	15 Optimise the IT infrastructure, resources and capabilities.	16 Reduce solution and service delivery defects and rework.	17 Protect [illegible]
Plan and Organise																	
PO1 Define a strategic IT plan.	✔	✔															
PO2 Define the information architecture.	✔			✔	✔						✔						
PO3 Determine technological direction.							✔								✔		
PO4 Define the IT processes, organisation and relationships.	✔	✔			✔												
PO5 Manage the IT investment.												✔					
PO6 Communicate management aims and direction.												✔	✔				
PO7 Manage IT human resources.					✔				✔								
PO8 Manage quality.			✔													✔	
PO9 Assess and manage IT risks.														✔			✔
PO10 Manage projects.	✔	✔															
Acquire and Implement																	
AI1 Identify automated solutions.	✔					✔											
AI2 Acquire and maintain application software.						✔	✔										
AI3 Acquire and maintain technology infrastructure.					✔			✔							✔		
AI4 Enable operation and use.			✔								✔		✔			✔	

Managing IT Resource to deliver IT Goals



COBIT as a Process Oriented Tool

Pengantar

- COBIT defines IT activities in a generic process model within four domains. These domains are
  1. **Plan and Organise,**
  2. **Acquire and Implement,**
  3. **Deliver and Support, and**
  4. **Monitor and Evaluate.**

  The domains map to IT's traditional responsibility areas of plan, build, run and monitor.
- The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities.
- Incorporating an operational model and a common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance.

PLAN AND ORGANISE (PO)

- This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.
- The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives.
- A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:
  - Are IT and the business strategy aligned?
  - Is the enterprise achieving optimum use of its resources?
  - Does everyone in the organisation understand the IT objectives?
  - Are IT risks understood and being managed?
  - Is the quality of IT systems appropriate for business needs?

ACQUIRE AND IMPLEMENT (AI)

- To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process.
- In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives.
- This domain typically addresses the following management questions:
  - Are new projects likely to deliver solutions that meet business needs?
  - Are new projects likely to be delivered on time and within budget?
  - Will the new systems work properly when implemented?
  - Will changes be made without upsetting current business operations?

DELIVER AND SUPPORT (DS)

- This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities.
- It typically addresses the followingmanagement questions:
  - Are IT services being delivered in line with business priorities?
  - Are IT costs optimised?
  - Is the workforce able to use the IT systems productively and safely?
  - Are adequate confidentiality, integrity and availability in place for information security?

MONITOR AND EVALUATE (ME)

- All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.
- This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It typically addresses the following management questions:
  - Is IT's performance measured to detect problems before it is too late?
  - Does management ensure that internal controls are effective and efficient?
  - Can IT performance be linked back to business goals?
  - Are adequate confidentiality, integrity and availability controls in place for information security?

Customizibility

- While most enterprises have defined plan, build, run and monitor responsibilities for IT, and most have the same key processes, few will have the same process structure or apply all 34 COBIT processes.
- COBIT provides a complete list of processes that can be used to verify the completeness of activities and responsibilities; however, they need not all apply, and, even more, they can be combined as required by each enterprise.

COBIT as a Control Based Approach

Control Based Approach

- COBIT defines control objectives for all 34 processes, as well as overarching process and application controls.
- Process 'need' controls!
- Effective controls *reduce risk*, increase the likelihood of *value delivery* and improve efficiency because there will be fewer errors and a more consistent management approach.

Controls

Kebijakan, prosedur, praktek dan struktur organisasi yang dirancang untuk menjamin agar business objective dapat tercapai, sehingga kejadian-kejadian yang tak diingikan dapat dicegah dan diperbaiki.

Control Objectives

Control objectives : "*statement of the desired result, or purpose to be archived by implementing control procedurs in a particular activity*"

IT control objectives provide a complete set of high-level requirements to be considered by management for effective control of each IT process. They:

- Are statements of managerial actions to increase value or reduce risk
- Consist of policies, procedures, practices and organisational structures
- Are designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected

Internal Controls (Kendali Internal)

- Internal control is a process put in place by the board of directors, senior management and all levels of personnel to provide reasonable assurance that an organization's business objectives will be achieved.

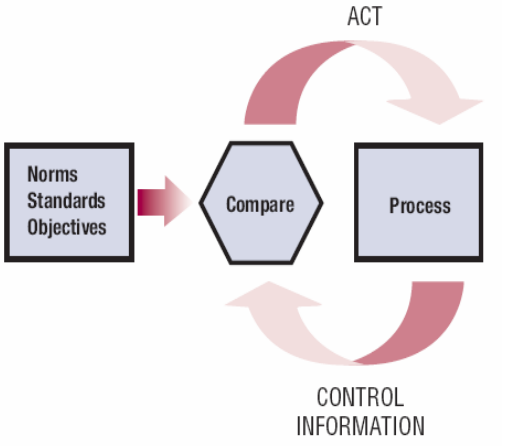
Controls & Control Objectives (5)

Contoh dari information systems control objectives :

1. Information on automated systems is secured from improper access
2. Each transaction is authorized and entered only once
3. All rejected transactions are reported.
4. Duplicate transactions are reported
5. Files are adequately backed up to allow for proper recovery

- The control objectives are identified by a two-character domain reference (PO, AI, DS and ME) plus a process number and a control objective number.

Control Model



When the room temperature (standard) for the heating system (process) is set, the system will constantly check (compare) ambient room temperature (control information) and will signal (act) the heating system to provide more or less heat.

DS5 Deliver and Support
Ensure Systems Security

Detailed Control Objectives

DS5 Ensure Systems Security

DS5.1 Management of IT Security
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan
Translate business information requirements, IT configuration, information risk action plans and information security culture into an overall IT security plan. The plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Security policies and procedures are communicated to stakeholders and users.

DS5.3 Identity Management
All users (internal, external and temporary) and their activity on IT systems (business application, system operation, development and maintenance) should be uniquely identifiable. User access rights to systems and data should be in line with defined and documented business needs and job requirements. User access rights are requested by user management, approved by system owner and implemented by the security-responsible person. User identities and access rights are maintained in a central repository. Cost-effective technical and procedural measures are deployed and kept current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management
Ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are addressed by user account management. An approval procedure outlining the data or system owner granting the access privileges should be included. These procedures should apply for all users, including administrators (privileged users), internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information are contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

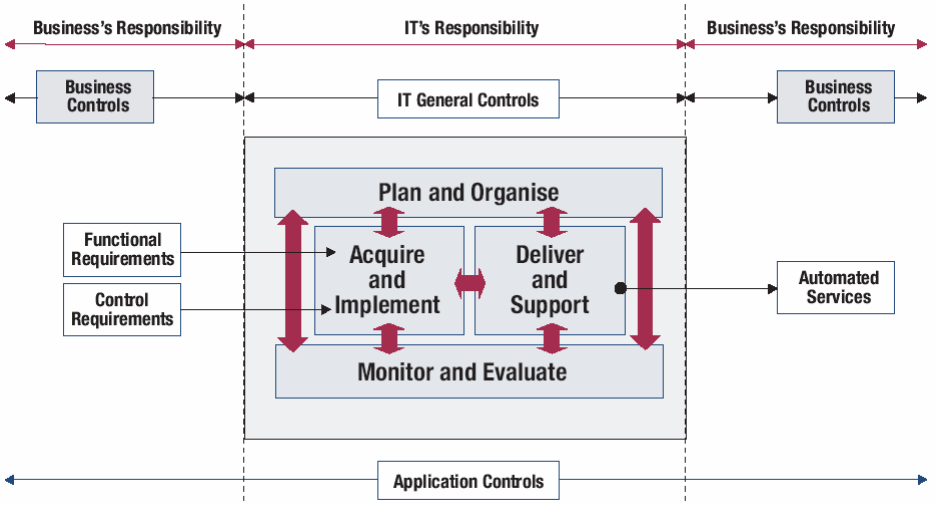
Internal Control Yang Berdampak Pada IT

1. Executive management level (yang kita pelajari selama ini)
2. Business process level
3. IT services

IT General & Application Control

- General controls are controls embedded in IT processes and services. Examples include:
  - Systems development
  - Change management
  - Security
  - Computer operations
- Controls embedded in business process applications are commonly referred to as application controls. Examples include:
  - Completeness
  - Accuracy
  - Validity
  - Authorisation
  - Segregation of duties

Boundaries of Business, General and Application Controls



Generic Control Requirements

- In addition to the control objectives, each COBIT process has generic control requirements that are identified by PCn, for process control number.
- They should be considered together with the process control objectives to have a complete view of control requirements.
  - PC1 Process Goals & Objective
  - PC2 Process Ownership
  - PC3 Process Repeatability
  - PC4 Roles & Responsabilities
  - PC5 Policy, Plan & Procedures
  - PC6 Process Performance Improvement

COBIT as a Measurement-Driven Approach

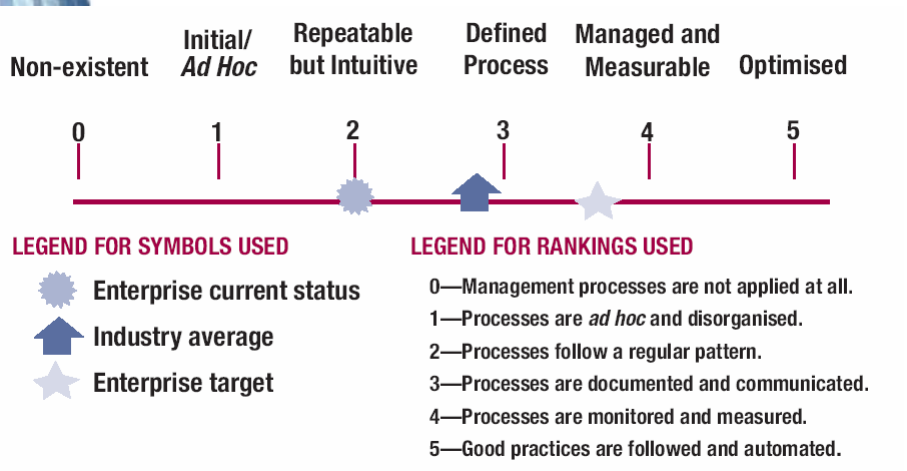
COBIT Provides:

1. Maturity models to enable benchmarking and identification of necessary capability improvements
2. Performance goals and metrics for the IT processes, demonstrating how processes meet business and IT goals and are used for measuring internal process performance based on balanced scorecard principles
3. Activity goals for enabling effective process performance

Maturity Models

- Maturity modelling for management and control over IT processes is based on a method of evaluating the organisation, so it can be rated from a maturity level of non-existent (0) to optimised (5).
- A generic definition is provided for the COBIT maturity scale, which is similar to CMM but interpreted for the nature of COBIT's IT management processes.
- The purpose of maturity model is to identify where issues are and how to set priorities for improvements.
- The purpose is *not to assess the level of adherence* to the control objectives.
- Process management capability *is not the same as process performance*.
- Capability may not always be the same across IT environment.

Graphical Representaiton of Maturity Models



Generic Maturity Models

0 Non-existent—Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.

1 Initial/ Ad Hoc—There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are *ad hoc* approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.

2 Repeatable but Intuitive—Processes have developed to the stage where similar procedures are followed by different people undertaking thesame task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined Process—Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.

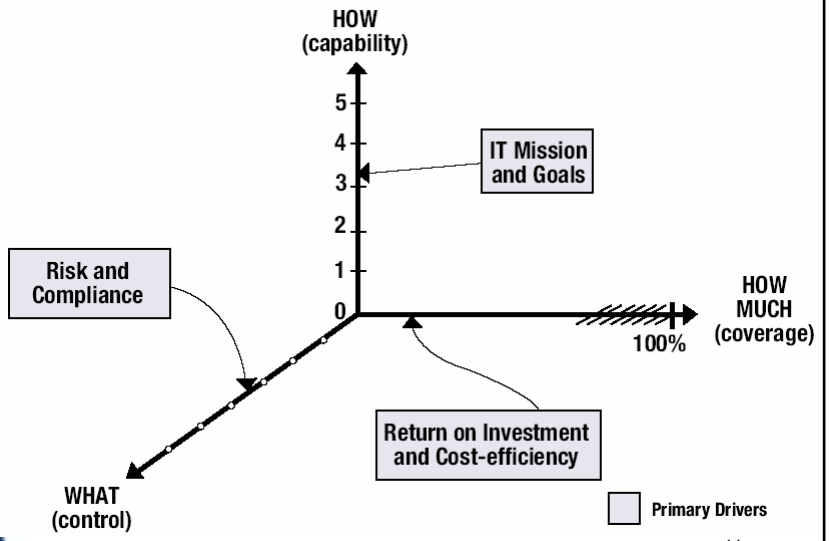
4 Managed and Measurable—Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimised—Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

Kapasitas Organisasi Mencapai Maturitas

- The maturity model is a way of measuring how well developed management processes are, i.e., how capable they actually are.
- How well developed or capable they should be primarily depends on the IT goals and the underlying business needs they support.
- *How much* of that *capability is actually deployed* largely depends on the return an enterprise wants from the investment.
  - For example, there will be critical processes and systems that need more and tighter security management than others that are less critical.
  - Bank butuh investasi TI dan kapabilitas TI lebih tinggi daripada KUD “Bibit, Pupuk dan Panen”
- On the other hand, the *degree and sophistication of controls* that need to be applied in a process are more driven by the enterprise’s *risk* appetite and applicable *compliance* requirements.

Tree Dimensions of Maturity



Capability Maturity Model

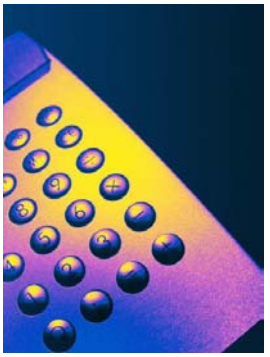
- The maturity model scales will help professionals explain to managers where IT process management shortcomings exist and set targets for where they need to be.
- The right maturity level will be influenced by the enterprise's business objectives, the operating environment and industry practices.
- Specifically, the level of management maturity will depend on the enterprise's dependence on IT, its technology sophistication and, most important, the value of its information.

	Awareness and Communication	Policies, Plans and Procedures	Tools and Automation	Skills and Expertise	Responsibility and Accountability	Goal Setting and Measurement
1	Recognition of the need for the process is emerging. There is sporadic communication of the issues.	There are *ad hoc* approaches to processes and practices. The process and policies are undefined.	Some tools may exist; usage is based on standard desktop tools. There is no planned approach to the tool usage.	Skills required for the process are not identified. A training plan does not exist and no formal training occurs.	There is no definition of accountability and responsibility. People take ownership of issues based on their own initiative on a reactive basis.	Goals are not clear and no measurement takes place.
2	There is awareness of the need to act. Management communicates the overall issues.	Similar and common processes emerge, but are largely intuitive because of individual expertise. Some aspects of the process are repeatable because of individual expertise, and some documentation and informal understanding of policy and procedures may exist.	Common approaches to use of tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even be shelfware.	Minimum skill requirements are identified for critical areas. Training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	An individual assumes his/her responsibility and is usually held accountable, even if this is not formally agreed. There is confusion about responsibility when problems occur, and a culture of blame tends to exist.	Some goal setting occurs; some financial measures are established but are known only by senior management. There is inconsistent monitoring in isolated areas.
3	There is understanding of the need to act. Management is more formal and structured in its communication.	Usage of good practices emerges. The process, policies and procedures are defined and documented for all key activities.	A plan has been defined for use and standardisation of tools to automate the process. Tools are being used for their basic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.	Skill requirements are defined and documented for all areas. A formal training plan has been developed, but formal training is still based on individual initiatives.	Process responsibility and accountability are defined and process owners have been identified. The process owner is unlikely to have the full authority to exercise the responsibilities.	Some effectiveness goals and measures are set, but are not communicated, and there is a clear link to business goals. Measurement processes emerge, but are not consistently applied. IT balanced scorecard ideas are being adopted, as is occasional intuitive application of root cause analysis.
4	There is understanding of the full requirements. Mature communication techniques are applied and standard communication tools are in use.	The process is sound and complete; internal best practices are applied. All aspects of the process are documented and repeatable. Policies have been approved and signed off on by management. Standards for developing and maintaining the processes and procedures are adopted and followed.	Tools are implemented according to a standardised plan, and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls.	Skill requirements are routinely updated for all areas, proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain experts are involved, and the effectiveness of the training plan is assessed.	Process responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. The IT balanced scorecard is implemented in some areas with exceptions noted by management and root cause analysis is being standardised. Continuous improvement is emerging.
5	There is advanced, forward-looking understanding of requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied, and integrated communication tools are in use.	External best practices and standards are applied. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end management and improvement.	Standardised tool sets are used across the enterprise. Tools are fully integrated with other related tools to enable end-to-end support of the processes. Tools are being used to support improvement of the process and automatically detect control exceptions.	The organisation formally encourages continuous improvement of skills, based on clearly defined personal and organisational goals. Training and education support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Process owners are empowered to make decisions and take action. The acceptance of responsibility has been cascaded down throughout the organisation in a consistent fashion.	There is an integrated performance measurement system linking IT performance to business goals by global application of the IT balanced scorecard. Exceptions are globally and consistently noted by management and root cause analysis is applied. Continuous improvement is a way of life.

Question

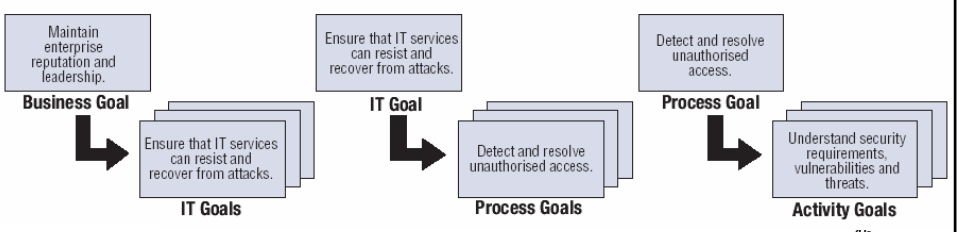
- Does higher COBIT maturity level always imply more sophisticated IT controls (i.e. split second backup means higher maturity level than weekly backup?

COBIT as a Performance Measurement Tool



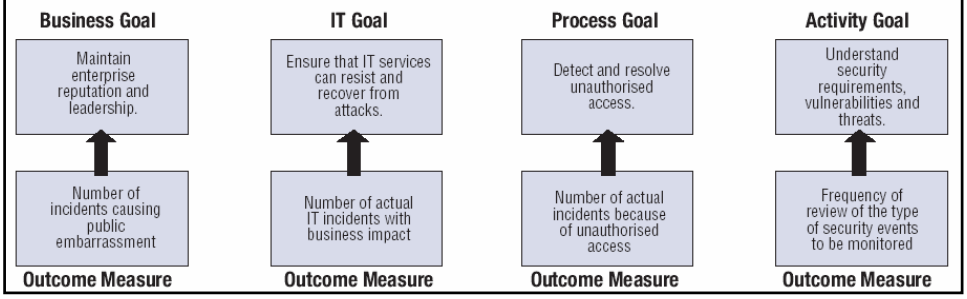
Goal Relationships

- IT goal is achieved by one process or the interaction of a number of processes.
- Therefore, IT goals help define the different process goals. In turn, each process goal requires a number of activities, thereby establishing the activity goals.
- Contoh:

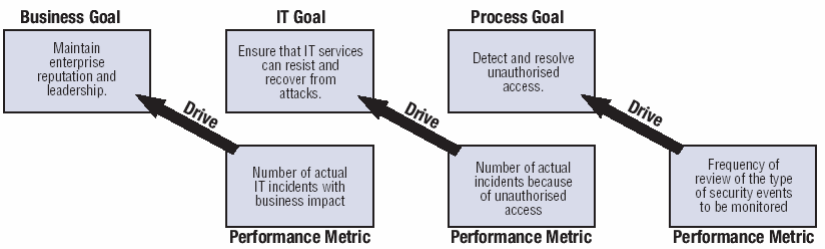


Metrics in COBIT

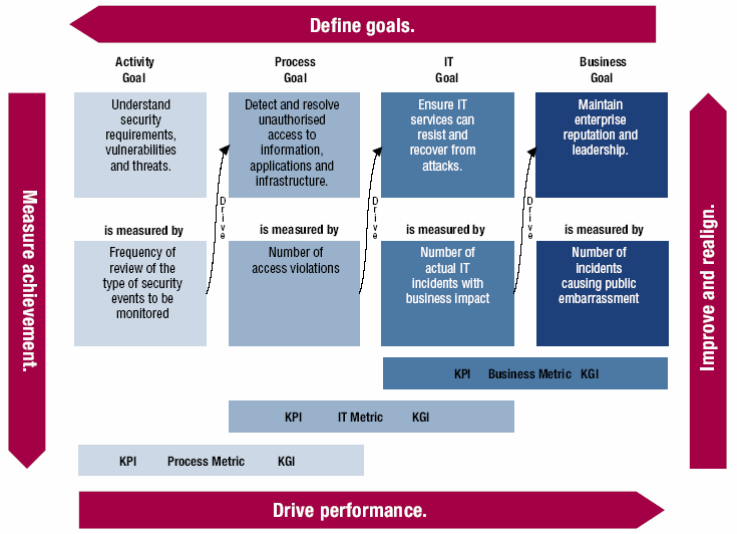
1. Outcome measures, previously key goal indicators (KGIs), indicate whether the goals have been met. These can be measured only after the fact and, therefore, are called '*lag indicators*'.
2. Performance indicators, previously key performance indicators (KPIs), indicate whether goals are likely to be met. They can be measured before the outcome is clear and, therefore, are called '*lead indicators*'. KPI will _drive_ higher level goals!



Performance Drivers



Contoh Hubungan Business Goal & IT Activity pada DS5- Ensure Systems Security

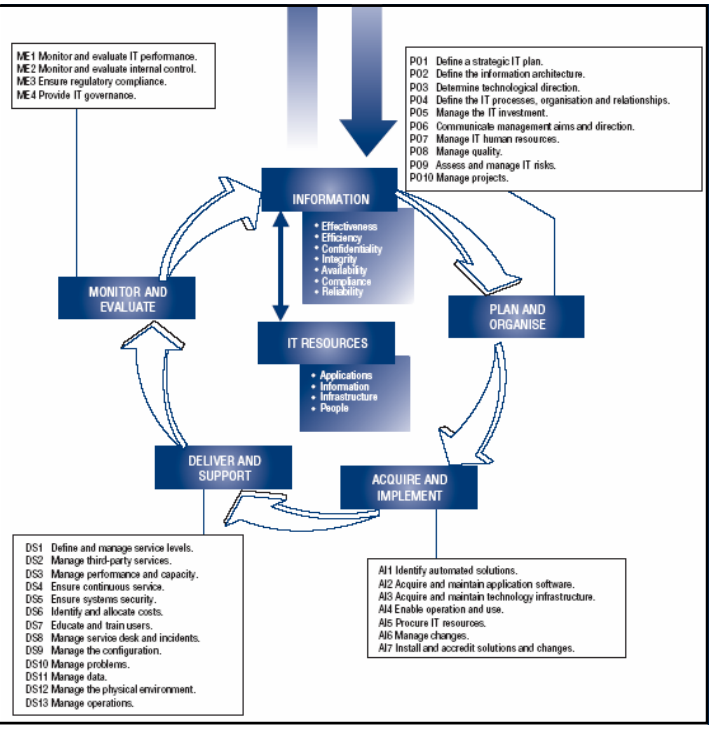


Catatan tentang implementasi COBIT

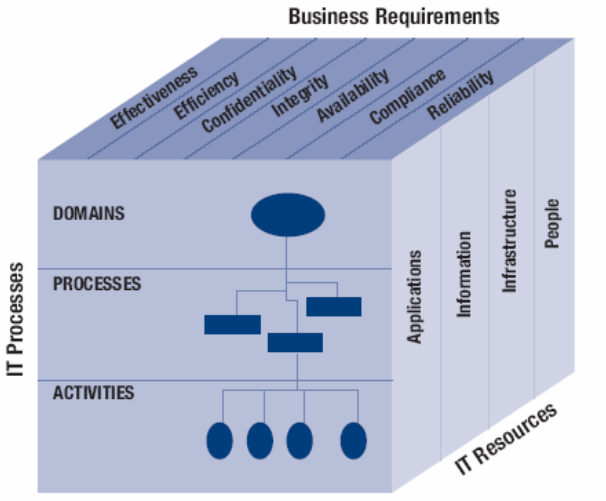
- Best practice is not the ultimate goal.
- Allow organizations to best determine which IT activities are important
- Kita bisa menganalisis IT process apa yang penting berdasarkan suatu inisatif strategic tertentu, misalnya rencana implementasi ERP, atau kebijakan strategic outsourcing.
- Bisa diselaraskan dengan IT Balanced Scorecard…!
- Karena fokusnya pada ‘requirement’ bukan pada ‘how-to’, maka COBIT sangat cocok untuk assessment.
- COBIT tidak memaksakan cara pengendalian teknis tertentu…!

The COBIT Framework

34 IT Process within COBIT 4.0



COBIT Cube



IT resources are managed by IT processes to achieve IT goals that respond to the business requirements.

COBIT Users

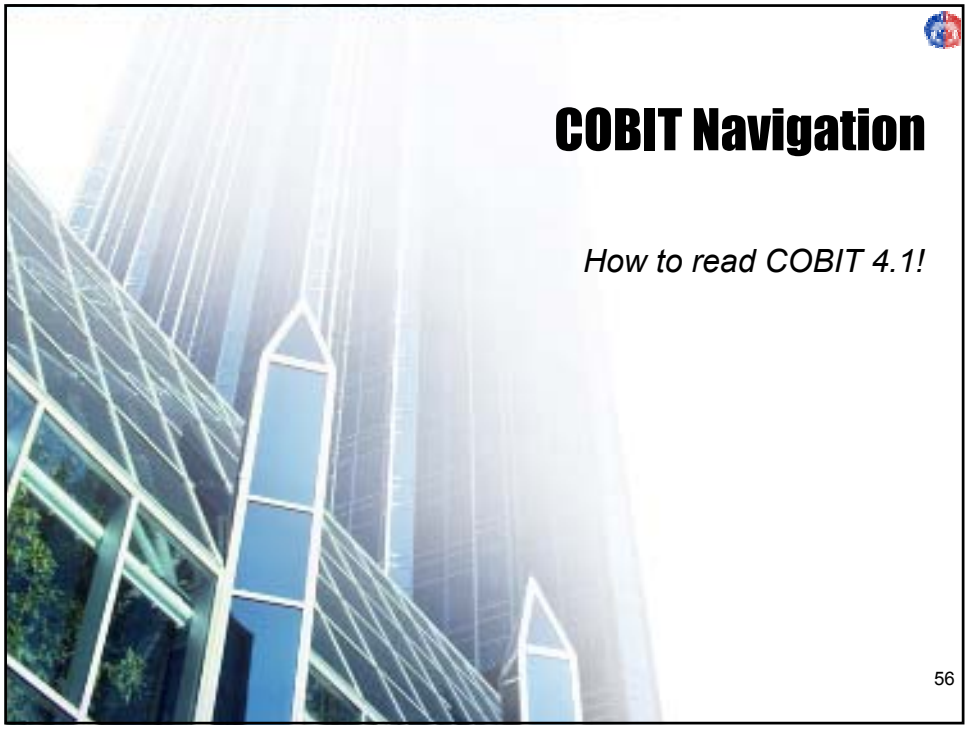
- **Executive management**—To obtain value from IT investments and balance risk and control investment in an often unpredictable IT environment
- **Business management**—To obtain assurance on the management and control of IT services provided by internal or third parties
- **IT management**—To provide the IT services that the business requires to support the business strategy in a controlled andmanaged way
- **Auditors**—To substantiate their opinions and/or provide advice to management on internal controls

How COBIT Framework Enables IT Governance Focus Areas

	Goals	Metrics	Practices	Maturity Models
Strategic alignment	P	P		
Value delivery		P	S	P
Risk management		S	P	S
Resource management		S	P	P
Performance measurement	P	P		S

P=Primary enabler S=Secondary enabler

Bagaimana dan contohnya apa?



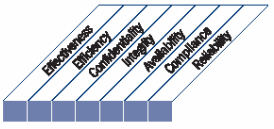
COBIT Navigation

How to read COBIT 4.1!

Components of COBIT

- Section 1 (**lihat halaman berikut**) contains a process description summarising the process objectives, with the process description represented in a waterfall. This page also shows the mapping of the process to the information criteria, IT resources and IT governance focus area.
  - "what the process owner needs to do"
- Section 2 contains the control objectives for this process.
- Section 3 contains the process inputs and outputs, RACI chart, goals and metrics.
  - "what the process owner needs from others"
  - "how should it be measured"
  - "what must be delegated and to whom?"
- Section 4 contains the maturity model for the process.
  - "what must be done to improve?"

Within each IT process, control objectives are provided as generic action statements of the minimum management good practices to ensure that the process is kept under control.



Control over the IT process of

process name

that satisfies the business requirement for IT of

summary of most important IT goals

by focusing on

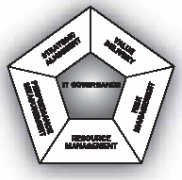
summary of most important process goals

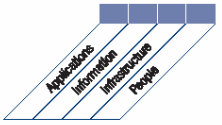
is achieved by

activity goals

and is measured by

key metrics





RACI Chart

The roles in the RACI chart are categorised for all processes as:

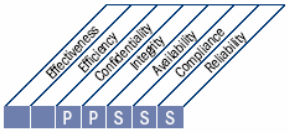
- Chief executive officer (CEO)
- Chief financial officer (CFO)
- Business executives
- Chief information officer (CIO)
- Business process owner
- Head operations
- Chief architect
- Head development
- Head IT administration (for large enterprises, the head of functions such as human resources, budgeting and internal control)
- The project management officer (PMO) or function
- Compliance, audit, risk and security (groups with control responsibilities but not operational IT responsibilities)

Deliver and Support
Ensure Systems Security
DS5

High-level Control Objective

DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilties, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.



Control over the IT process of

Ensure systems security

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

by focusing on

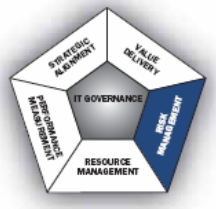
defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

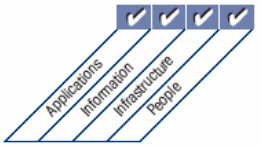
is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Testing security regularly

and is measured by

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties





DS5 **Deliver and Support**
Ensure Systems Security

CONTROL OBJECTIVES

DS5 Ensure Systems Security

DS5.1 Management of IT Security
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

DS5.2 IT Security Plan
Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

DS5.3 Identity Management
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

DS5.4 User Account Management
Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access

DS5 Ensure Systems Security

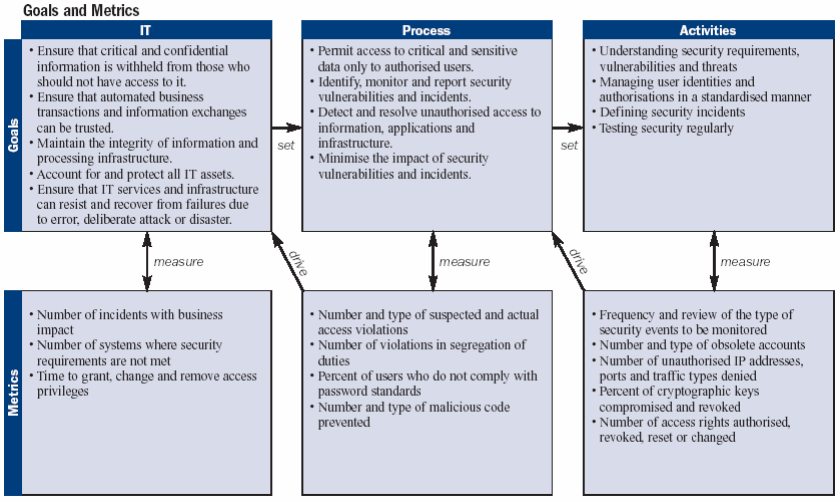
From	Inputs
PO2	Information architecture; assigned data classifications
PO3	Technology standards
PO9	Risk assessment
AI2	Application security controls specification
DS1	OLAs

Outputs	To
Security incident definition	DS8
Specific training requirements on security awareness	DS7
Process performance reports	ME1
Required security changes	AI6
Security threats and vulnerabilities	PO9
IT security plan and policies	DS11

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Define and maintain an IT security plan.	I	C	C	A	C	C	C	C	I	I	R
Define, establish and operate an identity (account) management process.			I	A	C	R	R	I			C
Monitor potential and actual security incidents.				A	I	R	C	C			R
Periodically review and validate user access rights and privileges.				I	A	C					R
Establish and maintain procedures for maintaining and safeguarding cryptographic keys.				A		R			I		C
Implement and maintain technical and procedural controls to protect information flows across networks.				A	C	C	R	R			C
Conduct regular vulnerability assessments.		I		A	I	C	C	C			R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.



Maturity Model

DS5 Ensure Systems Security

Management of the process of *Ensure systems security* that satisfies the business requirements for IT of *maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents* is:

0 Non-existent when
The organisation does not recognise the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process for IT security breaches. There is a complete lack of a recognisable system security administration process.

1 Initial/*Ad Hoc* when
The organisation recognises the need for IT security. Awareness of the need for security depends primarily on the individual. IT security is addressed on a reactive basis. IT security is not measured. Detected IT security breaches invoke finger-pointing responses, because responsibilities are unclear. Responses to IT security breaches are unpredictable.

2 Repeatable but Intuitive when
Responsibilities and accountabilities for IT security are assigned to an IT security co-ordinator, although the management authority of the co-ordinator is limited. Awareness of the need for security is fragmented and limited. Although security-relevant information is produced by systems, it is not analysed. Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate. IT security reporting is incomplete, misleading or not pertinent. Security training is available but is undertaken primarily at the initiative of the individual. IT security is seen primarily as the responsibility and domain of IT and the business does not see IT security as within its domain.

3 Defined when
Security awareness exists and is promoted by management. IT security procedures are defined and aligned with IT security policy. Responsibilities for IT security are assigned and understood, but not consistently enforced. An IT security plan and security solutions exist as driven by risk analysis. Reporting on security does not contain a clear business focus. *Ad hoc* security testing (e.g., intrusion testing) is performed. Security training is available for IT and the business, but is only informally scheduled and managed.

4 Managed and Measurable when
Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and procedures are completed with specific security baselines. Exposure to methods for promoting security awareness is mandatory. User identification, authentication and authorisation are standardised. Security certification is

Why is COBIT good for IT Governance?

- Simple, checklist based
- Common language for all level
- Template based, can be customized later
- Provides a maturity level, very good measure for benchmarking

Why must COBIT be cautiously used for IT Governance?

- Difficult to comprehend by business executives
- Not suited for strategic management of IT
- Generally it is a control based framework, doesn't tell you precisely *how* to do it!
- Even there are hows in COBIT, the 'hows' in COBIT are scattered around, does not create a holistic and complete picture and enough for reasoning.
- If not carefully understood, people tend to use it as a 'one-size-fits-all' solution.
- Doesn't tell you how to customize your IT Governance!
- Is not a tool to find root-cause of your IT problem.

Question

- Bagi yang pernah baca COBIT, apakah penjelasan di atas make sense?
- Apakah penjelasan COBIT yang anda barusan jelaskan mengubah persepsi anda tentang COBIT?

- TULISLAH:

"Apa persepsi anda dahulu terhadap COBIT (sebelum perkuliahan ini)"