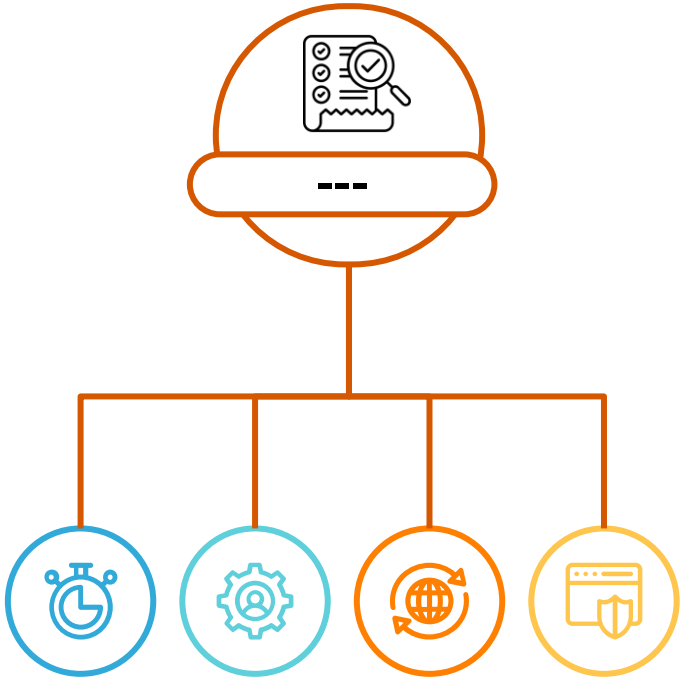
Audit dan Tata Kelola IT

Magister Tenik Informatika
Universitas Pamulang



Pertemuan 2
Kerangka Kerja Audit dan Tata Kelola TI

Audit menurut KBBI

1. *n* pemeriksaan pembukuan tentang keuangan (perusahaan, bank, dan sebagainya) secara berkala

2. *n* pengujian efektivitas keluar masuknya uang dan penilaian kewajaran laporan yang dihasilkannya

3. *n Komp* pemeriksaan terhadap peralatan, program, aktivitas, dan prosedur untuk menentukan efisiensi dari kinerja keseluruhan sistem terutama untuk menjamin integritas dan keamanan data

https://kbbi.kemdikbud.go.id/entri/audit

Pengertian Audit

Audit merupakan sebuah proses pengumpulan serta pemeriksaan bukti mengenai informasi guna menentukan dan membuat laporan terkait tingkat kesesuaian antara informasi dan kriteria yang ditetapkan. Audit ini harus dilaksanakan oleh orang yang kompeten dan independen.

(Arens, Alvin A., Elder, Randal J., Beasley, Mark S.. Auditing And Assurance Services: An Integrated Approach. 15 England: Pearson Education Limited, 2014.)

Pengertian Audit

Audit adalah pengumpulan dan dan penilaian bukti mengenai informasi untuk menentukan dan melaporakan mengenai tingkat kesesuaian antara informasi tersebut dengan ketentuan yang ditetapkan.

(American Accounting Association, Committee on Basic Auditing Concepts, dalam Robetson, 1990).

Referensi Tambahan di Channel LP3 UNPAM (Teori Audit dan Filosofinya) :
https://www.youtube.com/watch?v=yqCEVSSbfE8
https://www.youtube.com/watch?v=flA8d1K5HVo

Audit Internal

Audit internal adalah aktivitas independen, keyakinan obyektif, dan konsultasi yang dirancang untuk menambah nilai dan meningkatkan operasi organisasi. Audit internal ini membantu organisasi mencapai tujuannya dengan melakukan pendekatan sistematis dan disipilin untuk mengevaluasi dan meningkatkan efektifitas manajemen resiko, pengendalian, dan proses tata kelola.

(Solechan Achmad, Audit Sistem Informasi, Yayasan Prima Agus Teknik, Semarang, 2021)

Audit Internal

Sawyer (2005) mengemukakan definisi audit internal yang menggambarkan lingkup audit internal modern yang luas dan tak terbatas. Audit internal adalah sebuah penilaian yang sistematis dan objektif yang dilakukan auditor internal terhadap operasi dan kontrol yang berbeda-beda dalam organisasi untuk menentukan apakah :

- Informasi keuangan dan operasi telah akurat dan dapat diandalkan,
- Risiko yang dihadapi perusahaan telah diidentifikasi dan diminimalisasi,
- Peraturan eksternal serta kebijakan dan prosedur internal yang biasa diterima telah diikuti,
- Kriteria operasi yang memuaskan telah dipenuhi,
- Sumber daya telah digunakan secara efisien dan ekonomis, dan tujuan organisasi telah dicapai secara efektif --semua dilakukan dengan tujuan untuk dikonsultasikan dengan manajemen dan membantu anggota organisasi dalam menjalankan tanggung jawabnya secara efektif

(Solechan Achmad, Audit Sistem Informasi, Yayasan Prima Agus Teknik, Semarang, 2021)

Audit Eksternal

Audit eksternal adalah pemeriksaan yang dilakukan oleh akuntan independen. Di mana proses ini dilakukan untuk menghasilkan sertifikasi atas laporan keuangan yang dijalankan oleh suatu perusahaan. Nantinya, sertifikasi ini akan dibutuhkan oleh investor maupun pemberi modal untuk semua bisnis publik.

https://amt-it.com/blog/perbedaan-audit-internal-dan-eksternal/#Apa_Itu_Audit_Eksternal

Audit atas Sistem Informasi

Perlu dilakukan mengingat banyaknya risiko yang harus dihadapi oleh organisasi berkaitan dengan penggunaan teknologi informasi, antara lain:

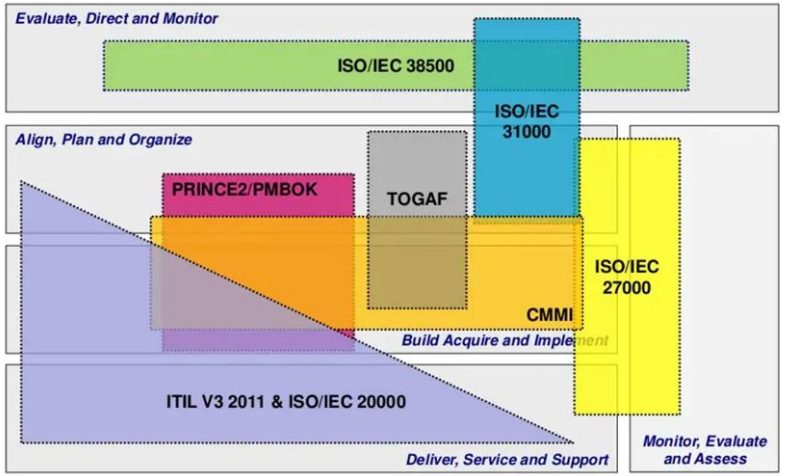
- Kehilangan data
- Kesalahan pengambilan keputusan
- Penyalahgunaan komputer
- Nilai investasi (pembengkakan)
- Aspek privasi
- Kesalahan pengoperasian komputer
- Evolusi teknologi

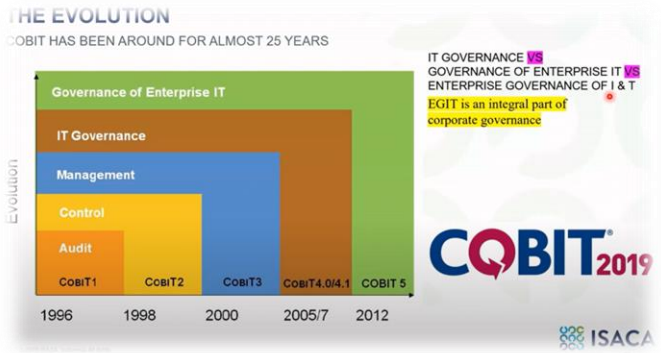
(Zuraidah, Eva., Budihartanti, Cahyani. Audit Sistem Informasi, Audit Sistem Informasi dan Manjemen menggunakan Cobit 4 dan 5, GRAHA ILMU, Yogyakarta, 2021)

Standar Auditor

- American Institute of Certified Public Accountants (AICPA)
- Institute of Internal Auditor (IIA)
- Internal Federation of Accountants (IFAC)
- Information Systems Audit and Control Association (ISACA)
- Ikatan Akuntan Indonesia (IAI)
- Ikatan Audit Sistem Informasi Indonesia (IASII)
- dst.

Governance
Tata Kelola





Pengertian Tata Kelola

Tata Kelola (*governance*) diartikan sebagai kombinasi proses dan struktur yang diterapkan oleh pimpinan organisasi untuk menginformasikan, mengarahkan, mengelola, dan memantau kegiatan organisasi dalam rangka pencapaian tujuan.

Tata Kelola bukanlah semata-mata hanya merupakan himpunan proses dan struktur yang berdiri sendiri, terpisah dari sistem lainnya. Tata kelola juga memiliki keterkaitan dengan manajemen risiko dan juga pengendalian internal.

Ref: Fariani, Elly, “Manajemen Risiko”, LAN-RI, 2020.

Pengertian Tata Kelola Pemerintahan

Menurut Bank Dunia (World Bank), good governance merupakan cara kekuasaan yang digunakan dalam mengelola berbagai sumber daya sosial dan ekonomi untuk pengembangan masyarakat (Mardoto, 2009).

Sedangkan menurut UNDP (United National Development Planning), good governance merupakan praktek penerapan kewenangan pengelolaan berbagai urusan penyelenggaraan negara secara politik, ekonomi dan administratif di semua tingkatan.

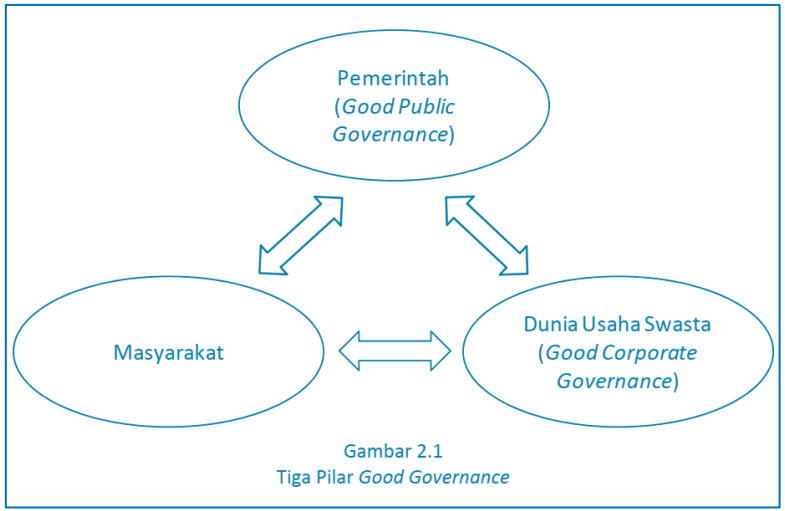
Ref: Tata Kelola, Manajemen Risiko, dan Pengendalian Intern, Pusdiklat BPKP, 2014.

Pengertian Tata Kelola Pemerintahan

Dalam konteks pembangunan, tata Kelola pemerintahan yang baik (*good government governance*) merupakan suatu mekanisme pengelolaan sumber daya ekonomi dan social untuk tujuan pembangunan nasional, sehingga penerapannya diharapkan akan menunjang terlaksananya pembangunan yang stabil secara efisien dan merata (*fair*). Hal ini karena penerapan tatakelola pemerintahan yang baik akan menyeimbangkan kepentingan dan pengaturan antara negara, pasar dan masyarakat.

Ref: Fariani, Elly, “Manajemen Risiko”, LAN-RI, 2020.

3 Domain Tata Kelola Pemerintahan



Tata Kelola, Manajemen Risiko, dan Pengendalian Intern, Pusdiklat BPKP, 2014

- Negara/pemerintahan sebagai pembuat kebijakan, pengedali, dan pengawas
- Swasta/dunia usaha sebagai penggerak aktivitas bidang ekonomi
- Masyarakat sebagai subjek dan objek dari sektor pemerintahan dan swasta

Ref: Fariani, Elly, “Manajemen Risiko”, LAN-RI, 2020.

Prinsip Tata Kelola Pemerintahan

- Partisipasi (Participation)
- Penegakan Hukum (Rule of Law)
- Transparansi (Transparency)
- Daya Tanggap (Responsiveness)
- Orientasi pada Kesepakatan (Consensus Orientation)
- Kesetaraan (Equity)
- Efektivitas dan Efisiensi (Effectiveness and Efficiency)
- Akuntabilitas (Accountability)
- Visi Strategis (Strategic Vision)

Catatan:
Tata Kelola IT untuk Pemerintahan akan dibahas selanjutnya pasa sesi SPBE

Ref: Tata Kelola, Manajemen Risiko, dan Pengendalian Intern, Pusdiklat BPKP, 2014.

IT Governance
(Tata Kelola TI)

Tata Kelola TI didefinisikan sebagai proses yang memastikan penggunaan TI yang efektif dan efisien dalam mendukung suatu organisasi untuk mencapai tujuannya.

Ref: https://www.gartner.com/en/information-technology/glossary/it-governance

IT Governance
(Tata Kelola TI)

ISO/IEC 38500:2015 : system by which the current and future use of IT is directed and controlled

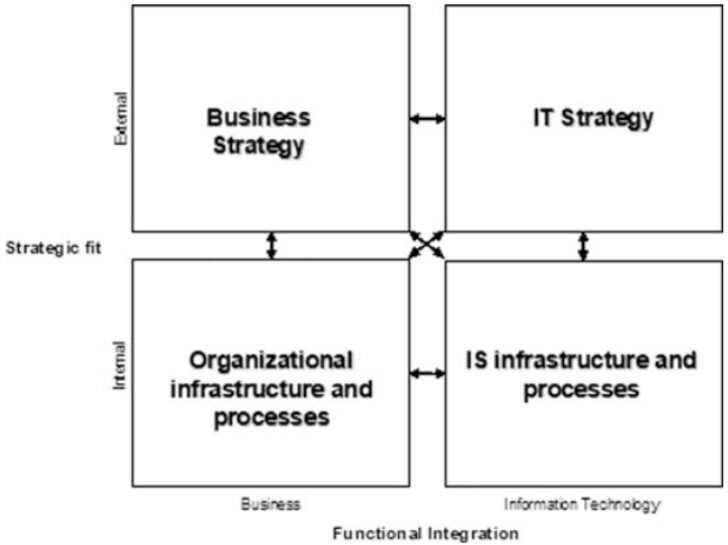
(sistem yang mana penggunaan TI saat ini dan masa depan diarahkan dan dikendalikan)

Enterprise Governance of IT
(Tata Kelola TI Korporasi/Perusahaan/Organisasi)

Tata Kelola TI Korporasi merupakan bagian integral dari tata kelola perusahaan yang, oleh karena itu, dewan bertanggung jawab. Ini melibatkan definisi dan implementasi proses, struktur, dan mekanisme relasional yang memungkinkan pemangku kepentingan bisnis dan TI untuk melaksanakan tanggung jawab mereka dalam mendukung **keselarasan bisnis/TI**, dan penciptaan serta perlindungan **nilai bisnis TI**.

Ref: De Haes S, Van Grembergen W, Joshi A, Huygh T. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, Third Edition, Springer Nature Switzerland AG, 2020. p.3.

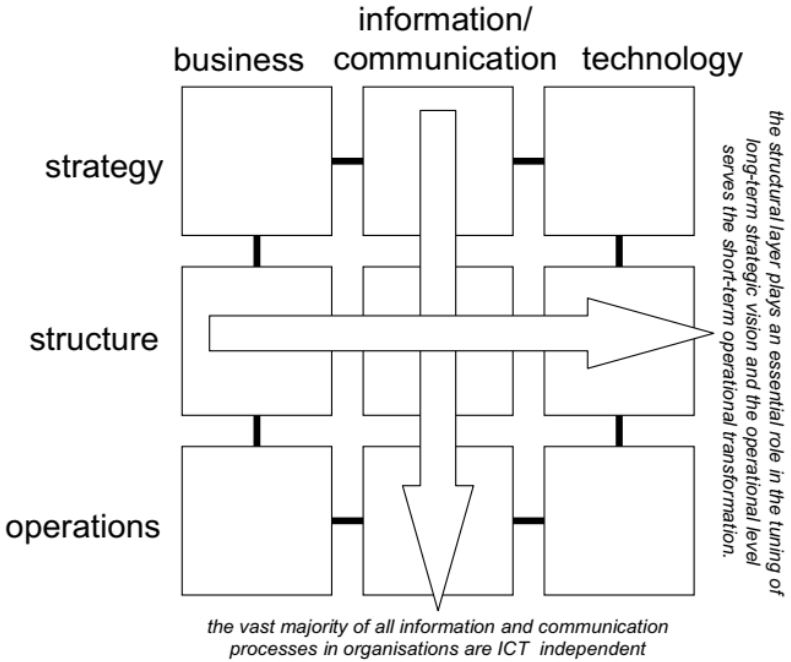
Strategic Alignment Model (SAM)



Henderson and Venkatraman (1993) were the first to clearly describe the interrelationship between business and IT in their well-known strategic alignment model (SAM)

Ref: De Haes S, Van Grembergen W, Joshi A, Huygh T. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, Third Edition, Springer Nature Switzerland AG, 2020. p.5.

Alignment framework of Maes
an extension of SAM (Maes, 1999)

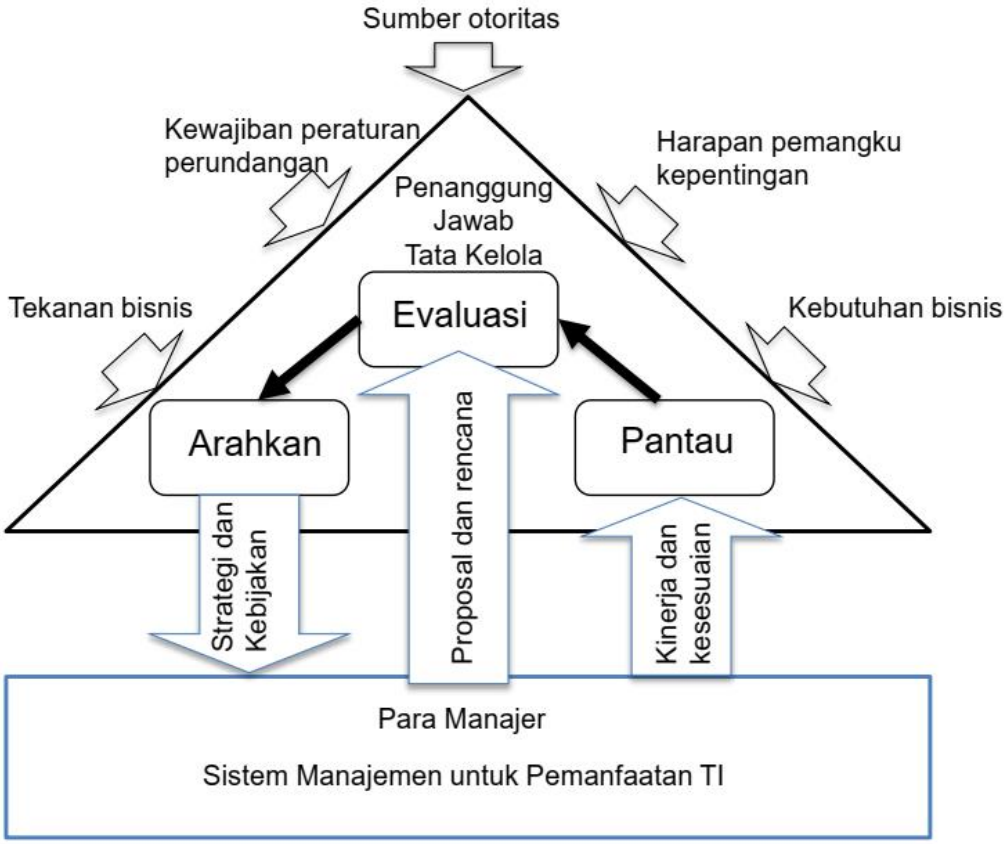


Ref: De Haes S, Van Grembergen W, Joshi A, Huygh T. Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations, Third Edition, Springer Nature Switzerland AG, 2020. p.7.

Framework IT Governance (Kerangka Kerja Tata Kelola TI)

- Control Objectives for Information and Related Technology (COBIT)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework
- Capability Maturity Model Integration (CMMI)
- International Organization for Standardization (ISO) / the International Electrotechnical Commission (IEC), (misalnya ISO/IEC 38500, ISO/IEC 31000, ISO/IEC 27000, 27001, 27002)
- IT Baseline Protection Manual
- ITSEC / Common Criteria
- Information Technology Infrastructure Library (ITIL)
- Project Management Body of Knowledge (PMBOK)
- Projects In Controlled Environments 2(PRINCE2)
- The Open Group Architecture Framework (TOGAF)
- VAL IT
- dst.

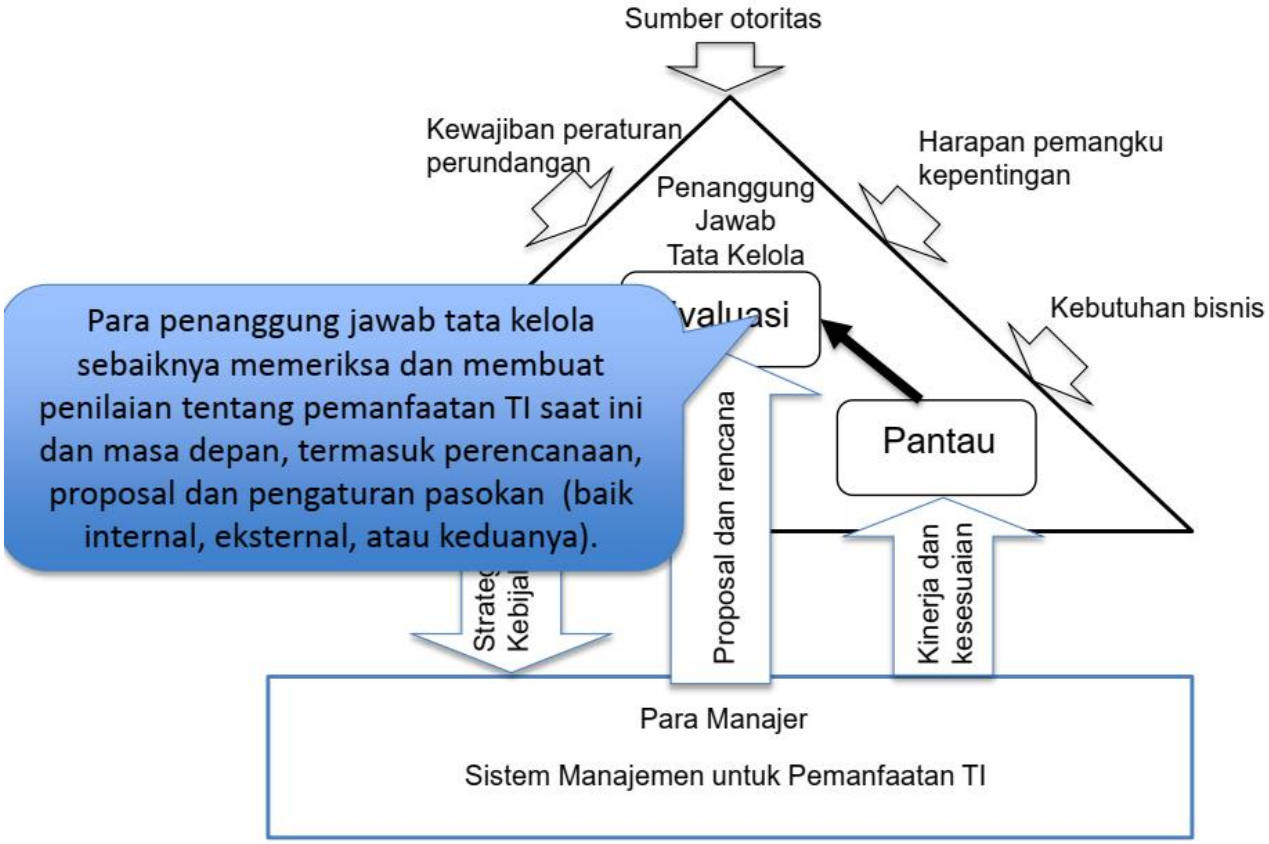
RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



Source: Figure 1 Model for Governance of IT, SNI ISO/IEC 38500:2015

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



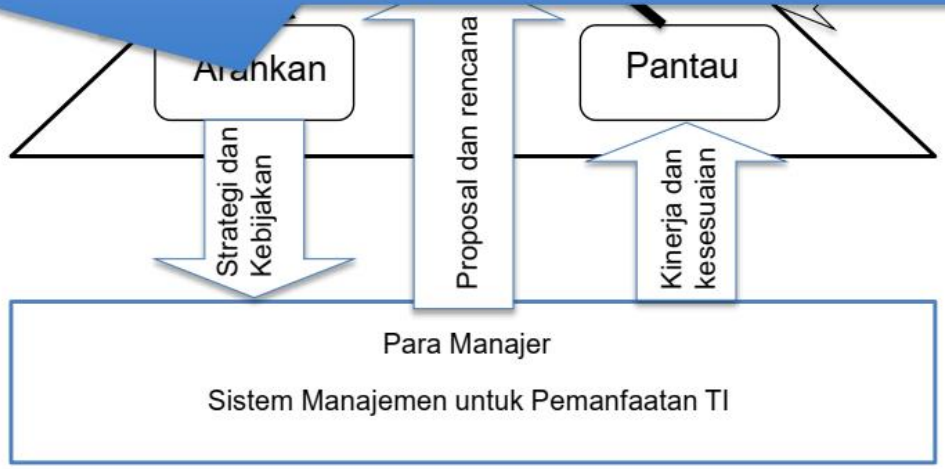
Source: Figure 1 Model for Governance of IT, SNI ISO/IEC 38500:2015

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi

Sumber otoritas

Para penanggung jawab tata kelola sebaiknya menetapkan tanggung jawab serta memberikan arahan atas penyusunan dan implementasi dari strategi dan kebijakan. Strategi sebaiknya menetapkan arah investasi TI dan apa yang harus dicapai TI. Kebijakan sebaiknya membentuk perilaku yang baik dalam pemanfaatan TI.



Source: Figure 1 Model for Governance of IT, SNI ISO/IEC 38500:2015

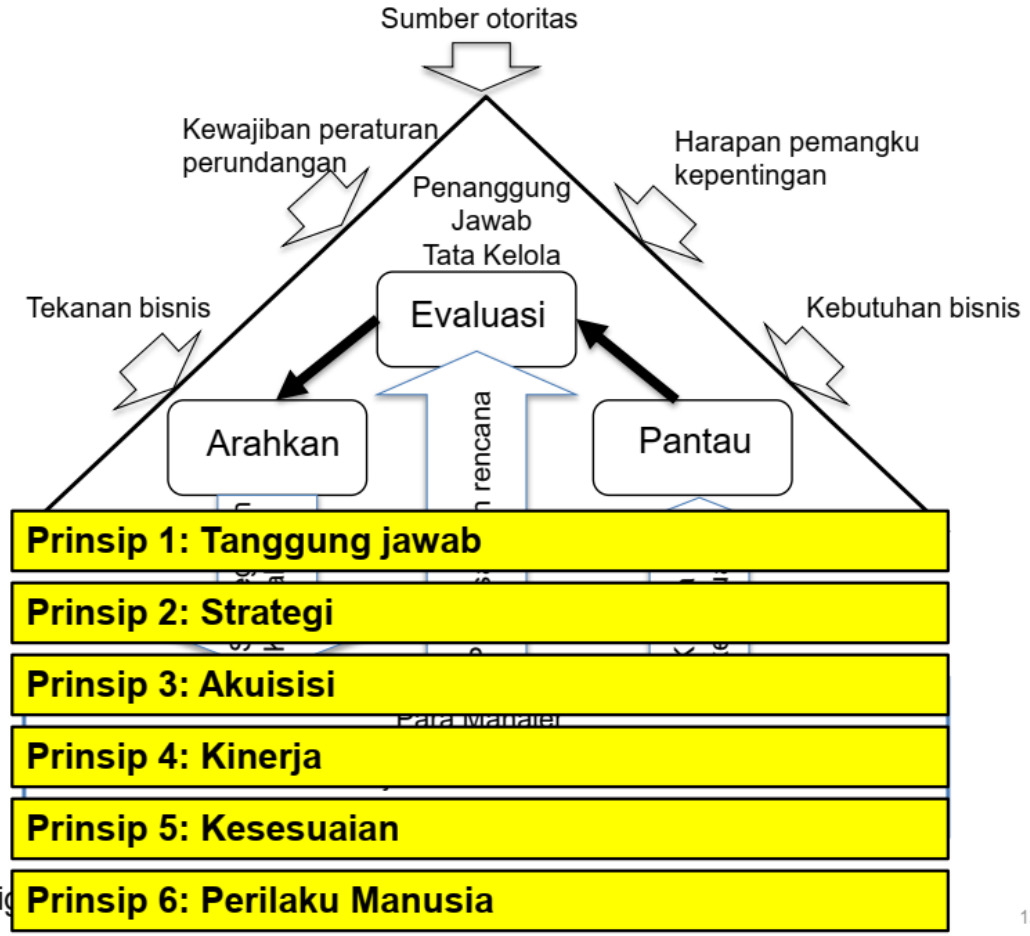
Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi

Source: Figure 1 Model for Governance of IT, SNI ISO/IEC 38500:2015

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

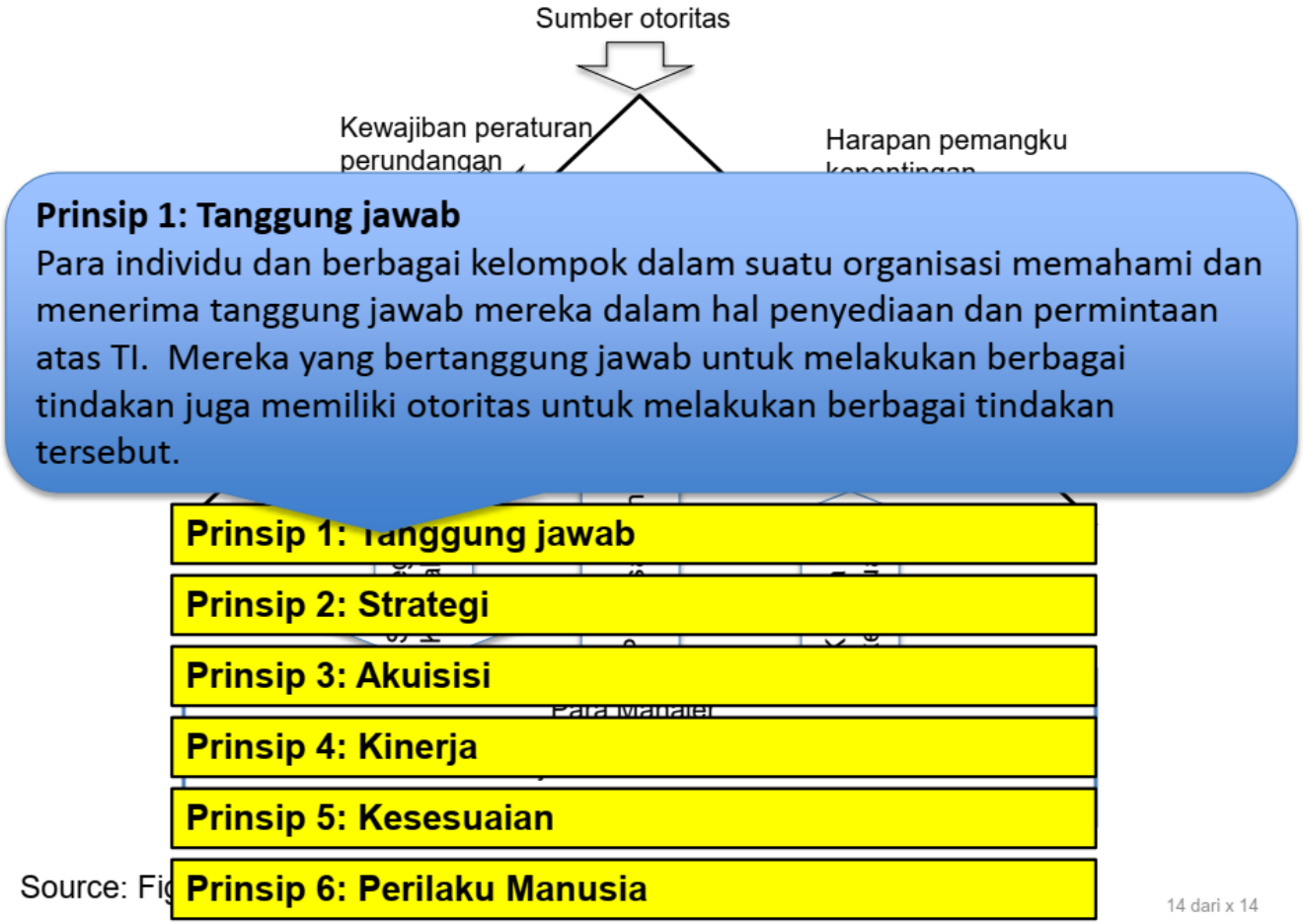
Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



Prinsip 1: Tanggung jawab

Para individu dan berbagai kelompok dalam suatu organisasi memahami dan menerima tanggung jawab mereka dalam hal penyediaan dan permintaan atas TI. Mereka yang bertanggung jawab untuk melakukan berbagai tindakan juga memiliki otoritas untuk melakukan berbagai tindakan tersebut.

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi

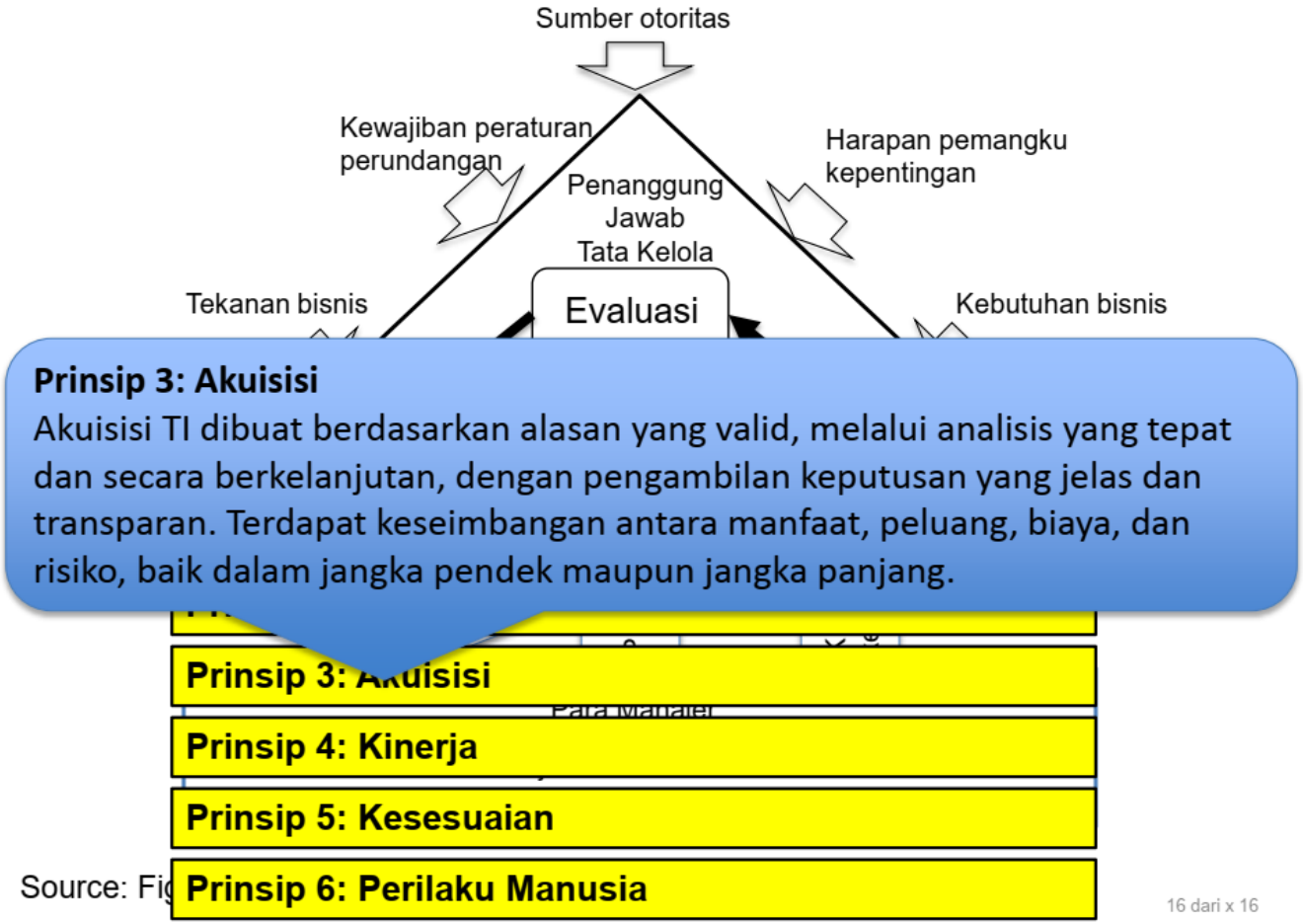
Prinsip 2: Strategi

Strategi bisnis organisasi memperhitungkan kemampuan TI saat ini dan di masa depan; rencana pemanfaatan TI memenuhi kebutuhan saat ini dan secara berkelanjutan dari strategi bisnis organisasi.

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



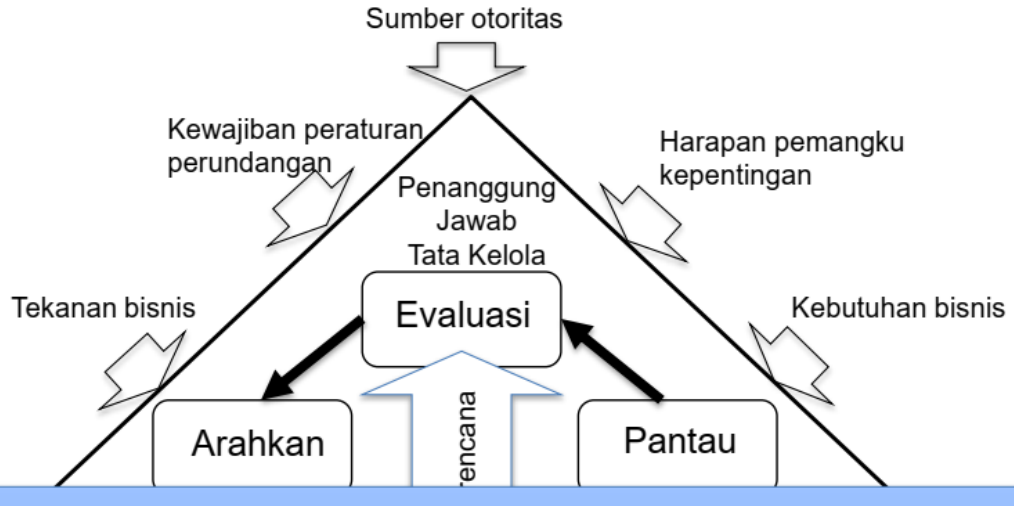
Prinsip 3: Akuisisi

Akuisisi TI dibuat berdasarkan alasan yang valid, melalui analisis yang tepat dan secara berkelanjutan, dengan pengambilan keputusan yang jelas dan transparan. Terdapat keseimbangan antara manfaat, peluang, biaya, dan risiko, baik dalam jangka pendek maupun jangka panjang.

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



Prinsip 4: Kinerja

TI digunakan untuk mendukung organisasi, menyediakan layanan, dengan tingkat layanan dan kualitas layanan yang diperlukan untuk memenuhi persyaratan bisnis saat ini dan di masa depan.

Prinsip 4: Kinerja

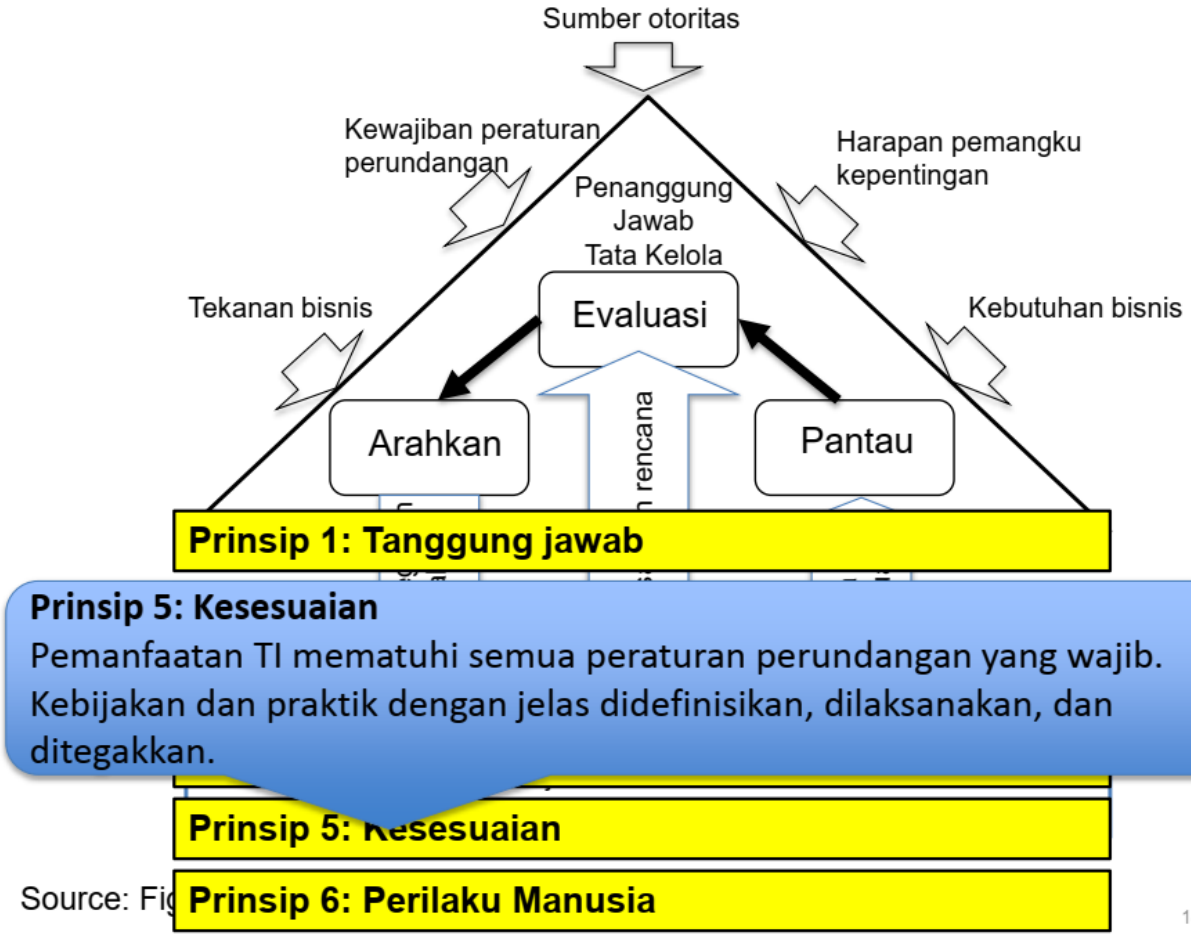
Prinsip 5: Kesesuaian

Prinsip 6: Perilaku Manusia

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



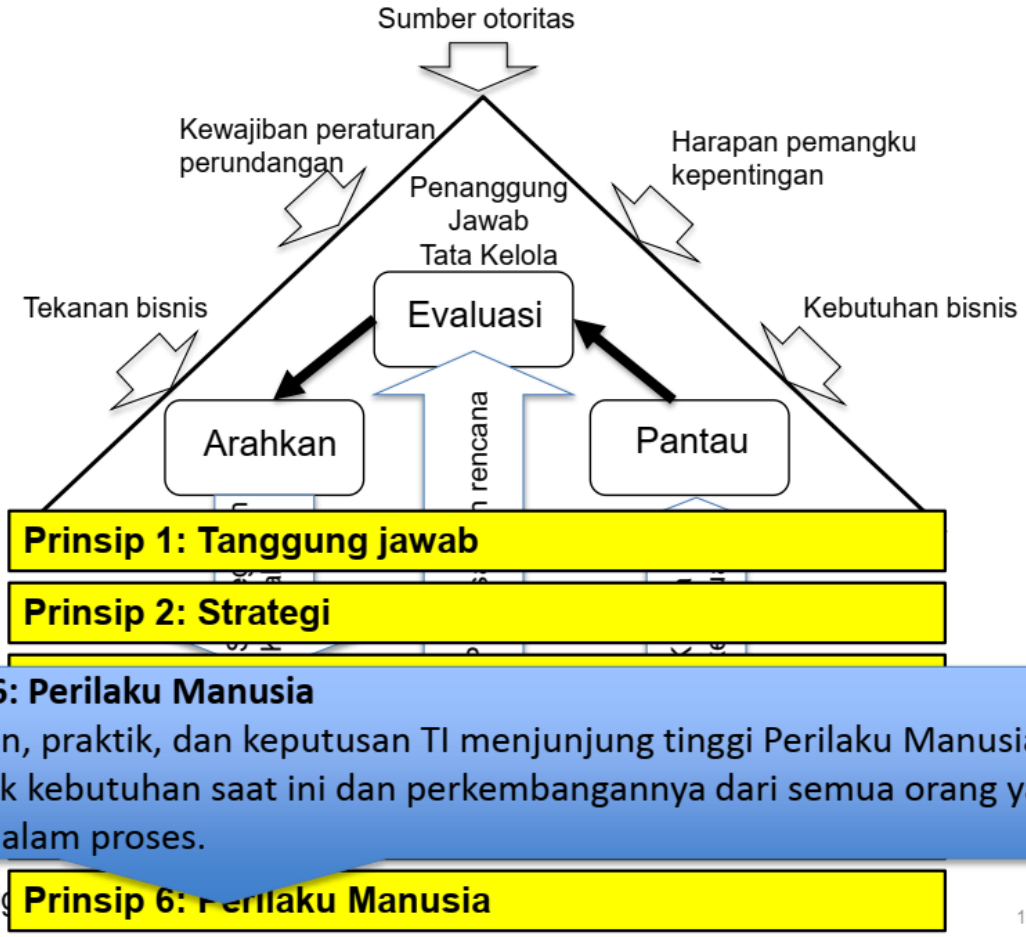
Prinsip 5: Kesesuaian

Pemanfaatan TI mematuhi semua peraturan perundangan yang wajib. Kebijakan dan praktik dengan jelas didefinisikan, dilaksanakan, dan ditegakkan.

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Enam Prinsip RSNI ISO/IEC 38500:2015 Tata Kelola Teknologi Informasi



Prinsip 6: Perilaku Manusia

Kebijakan, praktik, dan keputusan TI menjunjung tinggi Perilaku Manusia, termasuk kebutuhan saat ini dan perkembangannya dari semua orang yang terkait dalam proses.

Source: Fig

Ref: Sutikno, Sarwono. Teknologi informasi - Tata kelola TI untuk organisasi (ppt), 2015.

Pengertian Manajemen

Planning, building, running and monitoring of IT activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

What is COBIT???

COBIT is a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise.

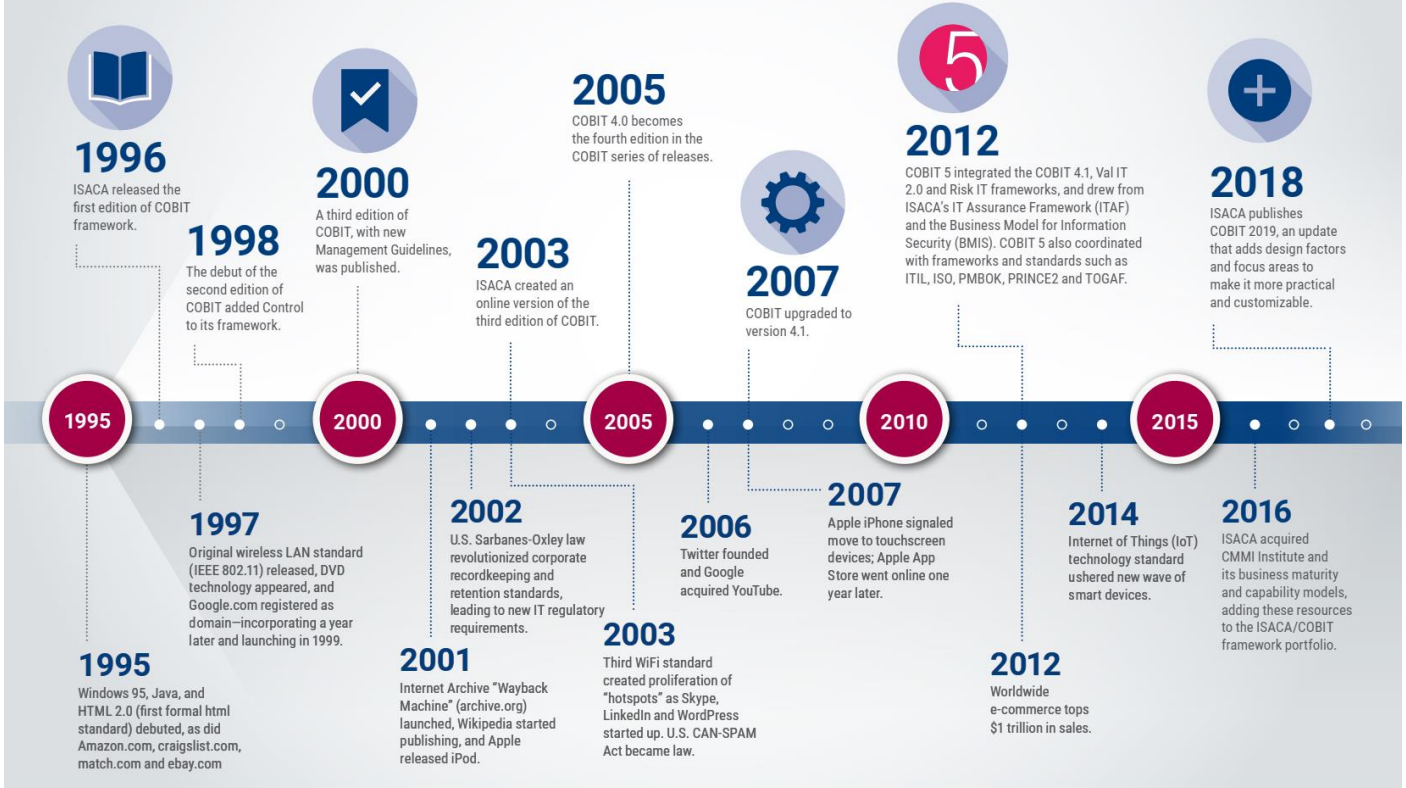
Enterprise I&T means all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise.

In other words, enterprise I&T is not limited to the IT department of an organization, but certainly includes it.

A HISTORICAL TIMELINE

The COBIT® Framework

COBIT 2019



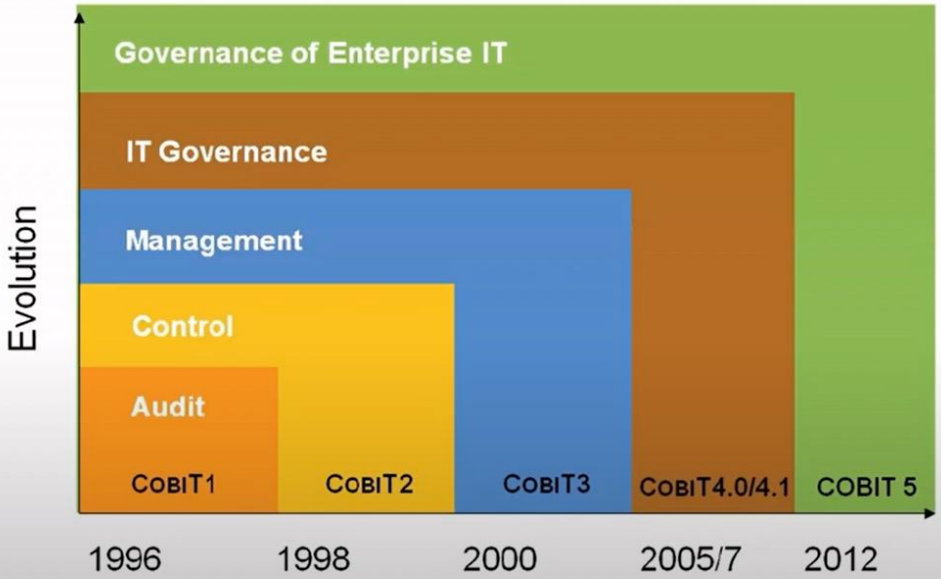
For more information, visit www.isaca.org/cobit

50 ISACA

COBIT Evolution

THE EVOLUTION

COBIT HAS BEEN AROUND FOR ALMOST 25 YEARS



IT GOVERNANCE VS
GOVERNANCE OF ENTERPRISE IT VS
ENTERPRISE GOVERNANCE OF I & T

EGIT is an integral part of
corporate governance

COBIT® 2019

ISACA Indonesia Chapter

Enterprise Governance of Information and Technology (EGIT) Context

Figure 1.1—The Context of Enterprise Governance of Information and Technology

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*, 2nd ed., Springer International Publishing, Switzerland, 2015, *https://www.springer.com/us/book/9783319145464*

Facts about COBIT

is

- COBIT is a framework for the GEIT, aimed at the whole enterprise.
- COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.
- COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system.
- COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

is not

- COBIT is not a full description of the whole IT environment of an enterprise.
- COBIT is not a framework to organize business processes.
- COBIT is not an (IT-)technical framework to manage all technology.
- COBIT does not make or prescribe any IT-related decisions. It will not decide what the best IT strategy is, what the best architecture is, or how much IT can or should cost. Rather, COBIT defines all the components that describe which decisions should be taken, and how and by whom they should be taken.

Governance Stakeholders (Internal)

Figure 2.1—COBIT Stakeholders	
Stakeholder	**Benefit of COBIT**
Internal Stakeholders	
Boards	Provides insights on how to get value from the use of I&T and explains relevant board responsibilities
Executive Management	Provides guidance on how to organize and monitor performance of I&T across the enterprise
Business Managers	Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for new strategic opportunities
IT Managers	Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.
Assurance Providers	Helps to manage dependency on external service providers, get assurance over IT, and ensure the existence of an effective and efficient system of internal controls
Risk Management	Helps to ensure the identification and management of all IT-related risk

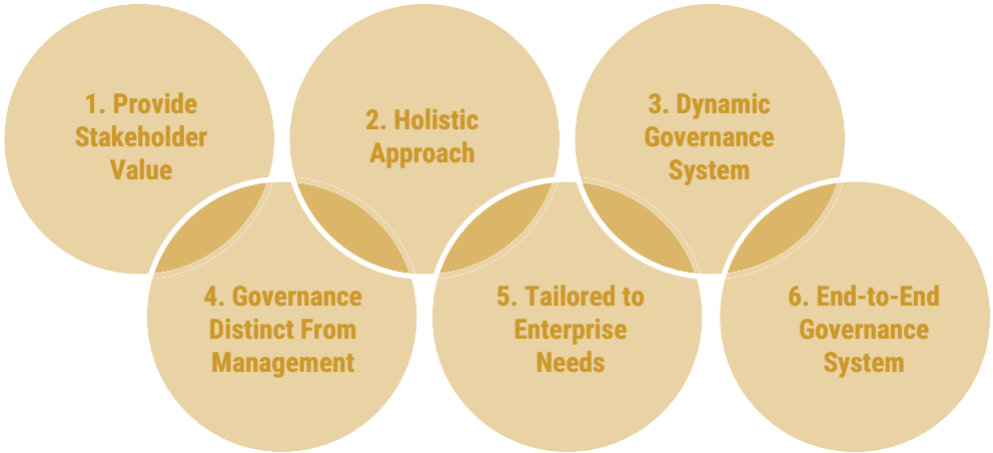
Governance Stakeholders (External)

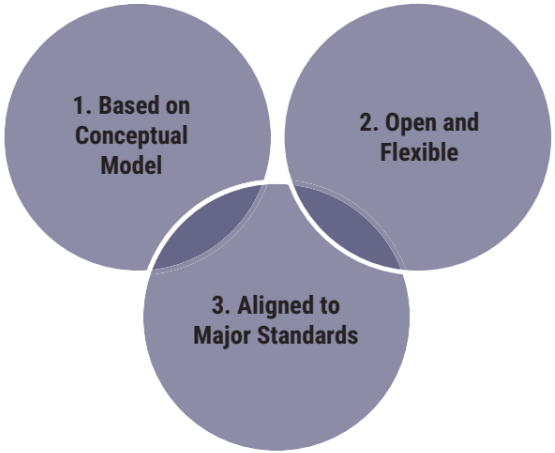
Figure 2.1—COBIT Stakeholders	
Stakeholder	**Benefit of COBIT**
External Stakeholders	
Regulators	Helps to ensure the enterprise is compliant with applicable rules and regulations and has the right governance system in place to manage and sustain compliance
Business Partners	Helps to ensure that a business partner's operations are secure, reliable and compliant with applicable rules and regulations
IT Vendors	Helps to ensure that an IT vendor's operations are secure, reliable and compliant with applicable rules and regulations

COBIT Principles

governance system principles

governance framework principles





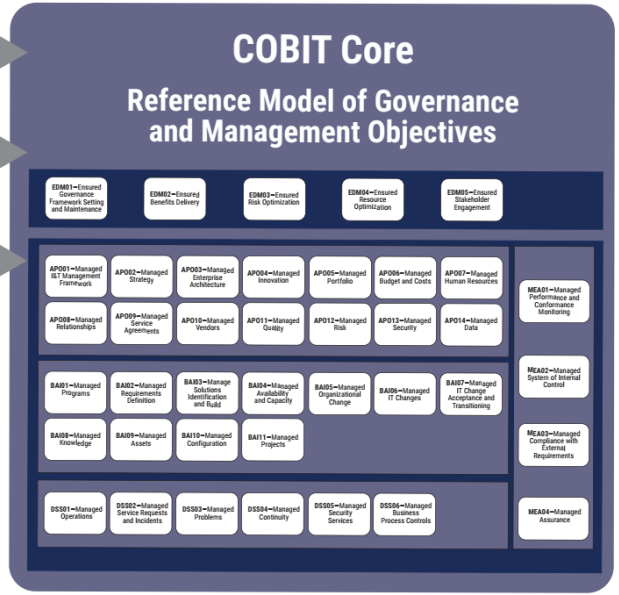
Inputs to COBIT® 2019

COBIT 5

Standards, Frameworks, Regulations

Community Contribution

COBIT® 2019



- Enterprise strategy
- Enterprise goals
- Enterprise size
- Role of IT
- Sourcing model for IT
- Compliance requirements
- Etc.

Design Factors

Focus Area

- SME
- Security
- Risk
- DevOps
- Etc.

Tailored Enterprise Governance System for Information and Technology

- Priority governance and management objectives
- Specific guidance from focus areas
- Target capability and performance management guidance

COBIT Core Publications

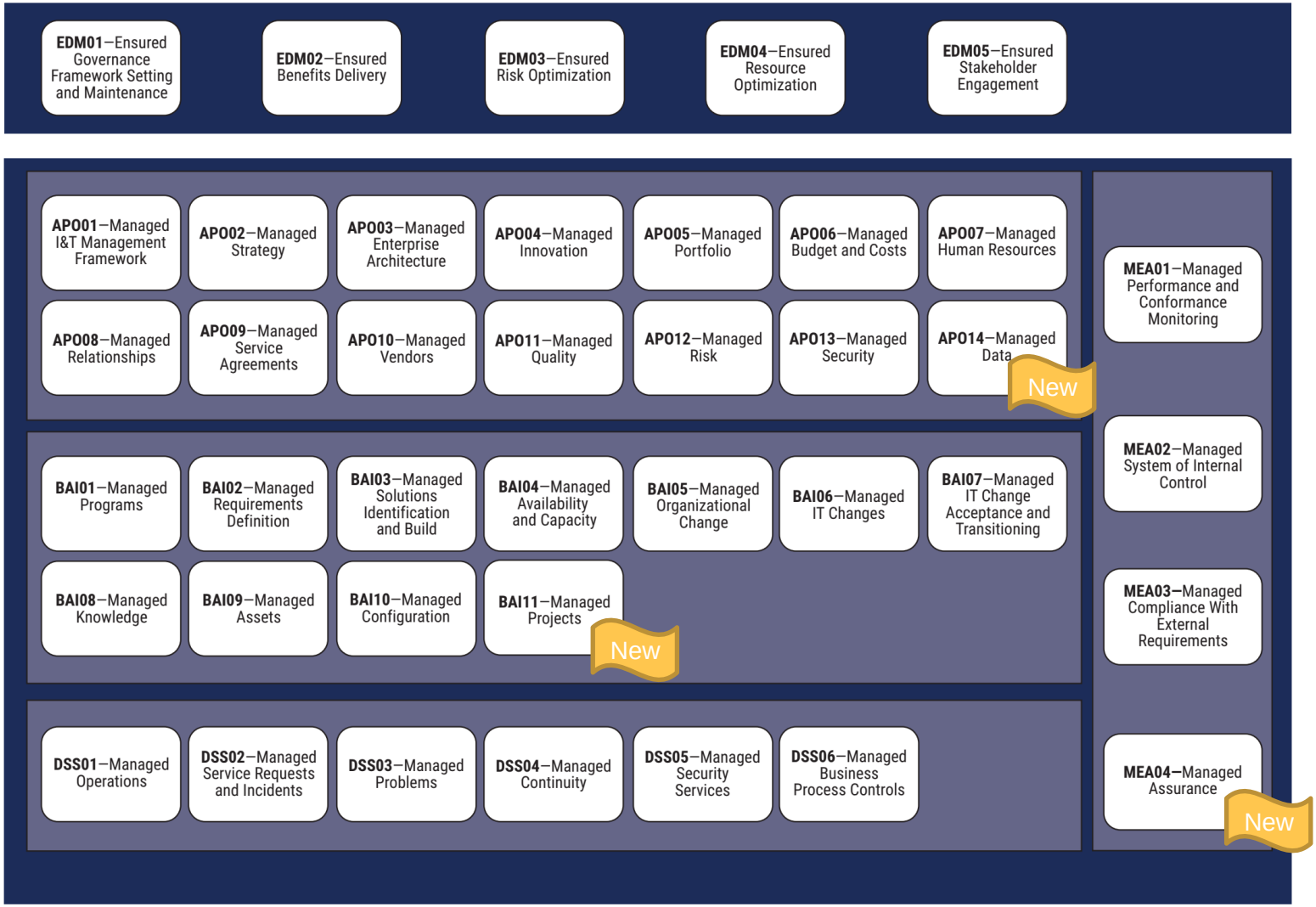
COBIT® 2019 Framework: Introduction and Methodology

COBIT® 2019 Framework: Governance and Management Objectives

COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution

COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution

COBIT 2019 Core Model



Governance and Management Objectives in COBIT

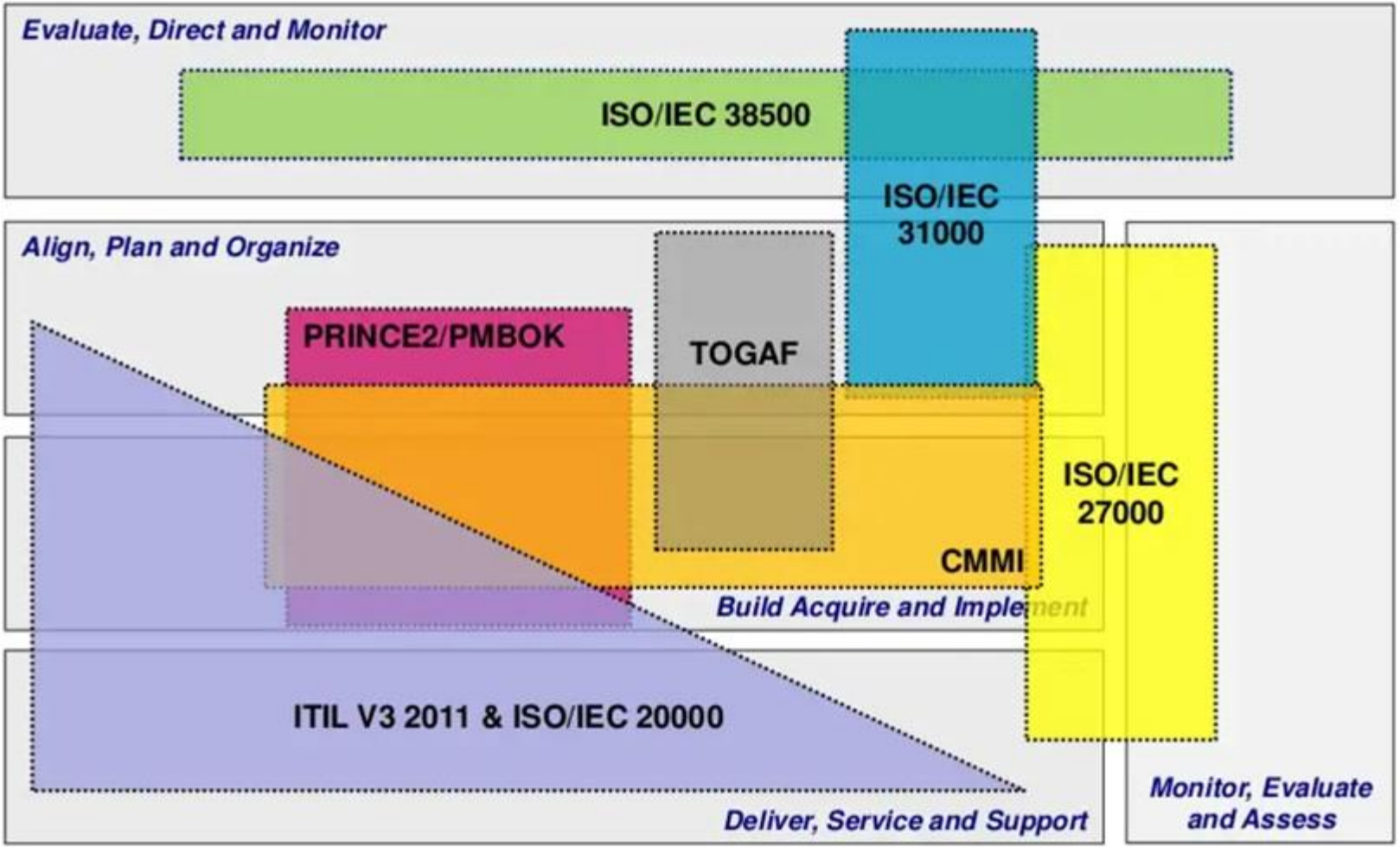
Governance objectives are grouped in the **Evaluate, Direct and Monitor (EDM)** domain.

In EDM domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.

Governance and Management Objectives in COBIT

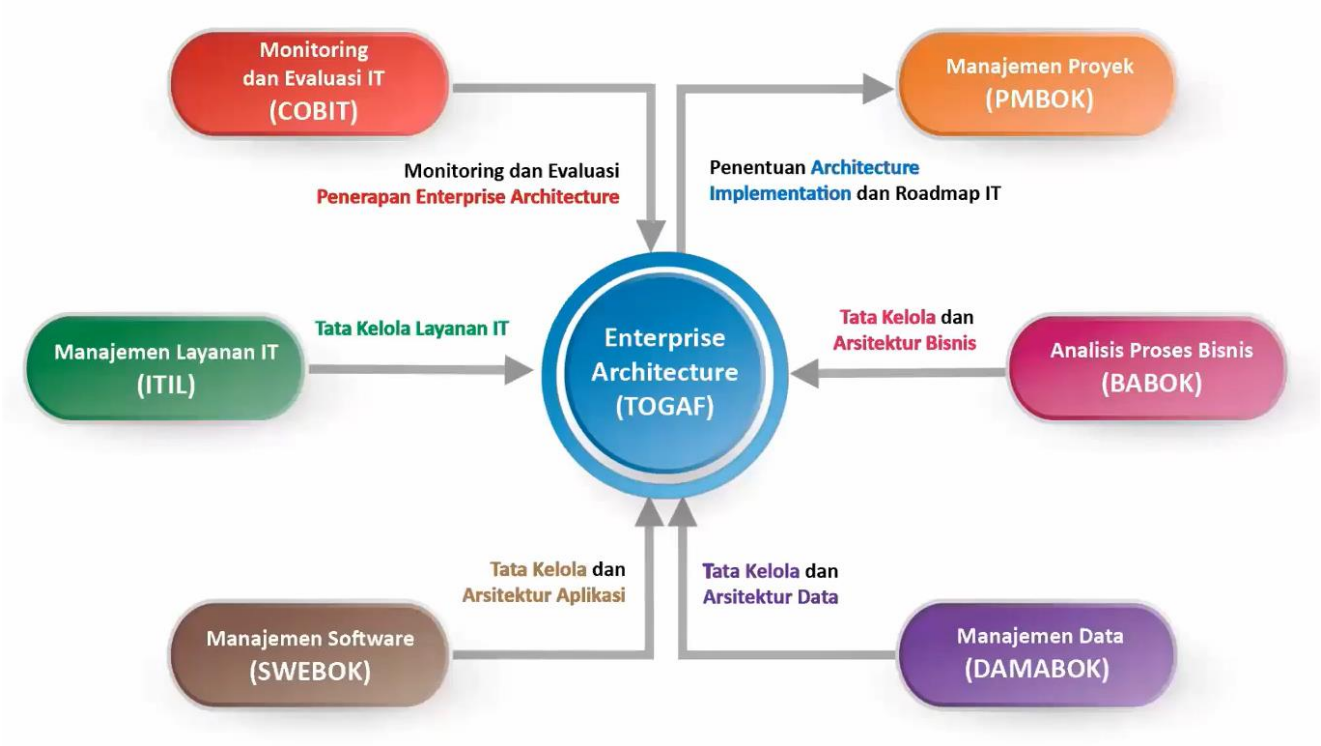
Management objectives are grouped in four domains

- **Align, Plan and Organize** (APO) addresses the overall organization, strategy and supporting activities for I&T.
- **Build, Acquire and Implement** (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
- **Deliver, Service and Support** (DSS) addresses the operational delivery and support of I&T services, including security.
- **Monitor, Evaluate and Assess** (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external req



https://www.ventasporpasos.com/2021/09/gerente-de-tecnologia-cual-es-la.html

Relationship



https://www.youtube.com/watch?v=X_7-l26nwBY