ISOCENTER INDONESIA

The Ultimate ISO and Management System Resources.

Meningkatkan Keselarasan Strategi TI dengan Strategi Bisnis Korporasi Menggunakan Pendekatan COBIT 2019

Dalam Konteks Memahami Pedoman Tata Kelola TI berdasarkan PER-2/MBU/03/2023

Roni Sulistyo Sutrisno

Bagian I

Apa dan Mengapa Keselarasan Strategi TI dengan Strategi Bisnis Perusahaan

Studi Kasus Ketidakselarasan Strategi (1): Kegagalan Implementasi Eenterprise Resource Planning (ERP)

Dari internet mudah ditemukan *real case study* kegagalan penerapan ERP pada Tahun 1990-an hingga 2000-an yang terutama disebabkan oleh:

- Penerapan ERP tidak didasarkan atas *digitalization roadmap* yang mengikuti kebutuhan bisnis, namun lebih kepada “mengikuti trend transformasi digital”.
- Anggapan bahwa ERP dapat menyelesaikan semua masalah produktifitas.
- Belum dilakukan pemetaan kematangan organisasi dalam mengadopsi inisiatif-inisiatif digitalisasi.
- Mengesampingkan manajemen proses bisnis dan hanya berfokus kepada *business process automation*.
- Mengabaikan manajemen perubahan (*change management*) dan hanya berfokus kepada masalah teknis (*develop & deploy*).

Studi Kasus Ketidakselarasan Strategi (2):

Implementasi Solusi TI yang Justru Menurunkan Produktivitas

Dari internet (lagi-lagi) mudah ditemukan *real case study* penerapan Solusi TI yang justru kontra produktif, yang disebabkan oleh:

- Tidak benar-benar mengetahui apa kebutuhan Solusi TI yang "*fit for purpose*".
- Tidak memiliki rencana strategis TI (yang efektif), sehingga keputusan penerapan Solusi TI yang lebih kepada sesuatu yang reaktif daripada proaktif.
- "Tergoda" oleh solusi yang ditawarkan oleh penyedia Solusi TI.
- Selalu mencari Solusi termurah, tanpa memahami nilai yang diharapkan dari sebuah Solusi TI.
- Tidak mengetahui bagaimana cara pengawasan yang paling tepat dalam akuisisi Solusi TI.

Harapan Pemangku Kepentingan Terhadap TI

- Mencapai **Efektivitas**
- Memberdayakan **Manusia**
- Meningkatkan **Efisiensi**
- Menerapkan **Transparansi**
- Mengintegrasikan **Organisasi**
- Mengoptimalkan **Sumber Daya**
- Memenuhi **Standar Aturan**
- Mempercepat **Proses**
- Memaksimalkan **Pelayanan**
- Memperbaiki **Kualitas**
- Mengurangi **Biaya**
- Memuaskan **Pelanggan**
- Menciptakan **Inovasi**
- Mempermudah **Aktivitas**

… dan lain sebagainya.

Kenyataan yang Dihadapi….

- ❑Perkembangan Cepat
- ❑Ketergantungan Pihak Ketiga
- ❑Biaya Tinggi
- ❑Kompetensi SDM Rendah
- ❑Proyek Terlambat
- ❑Arsitektur Kompleks
- ❑Sistem Kadaluwarsa
- ❑Kapabilitas Terbatas
- ❑Tidak Auditable
- ❑Implementasi Tambal Sulam
- ❑Tidak Sesuai Kebutuhan
- ❑Perubahan Kebutuhan

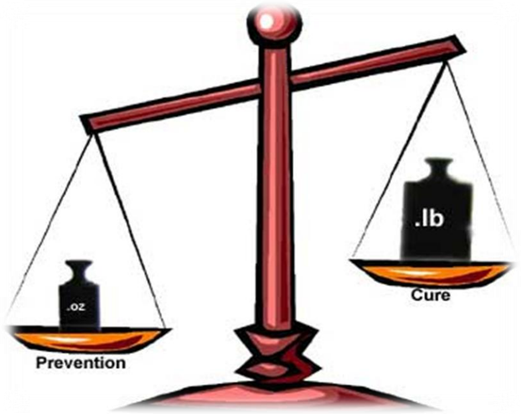
… dan lain sebagainya.

Kecenderungan…

Kenyataan
BIAYA + RESIKO

>

Harapan akan
MANFAAT



…baik yang bersifat **TANGIBLE** maupun **INTANGIBLE** !

Alasan Lain….

TRANSFORMASI DIGITAL

Digitalisasi ebagai Alat Bantu → Support

“Aktifitas Terbantu”

Digitalisasi Sebagai Enabler Proses Bisnis → Otomasi

“Produktifitas Terbantu”

Digitalisasi Sebagai Enabler Bisnis → New Value

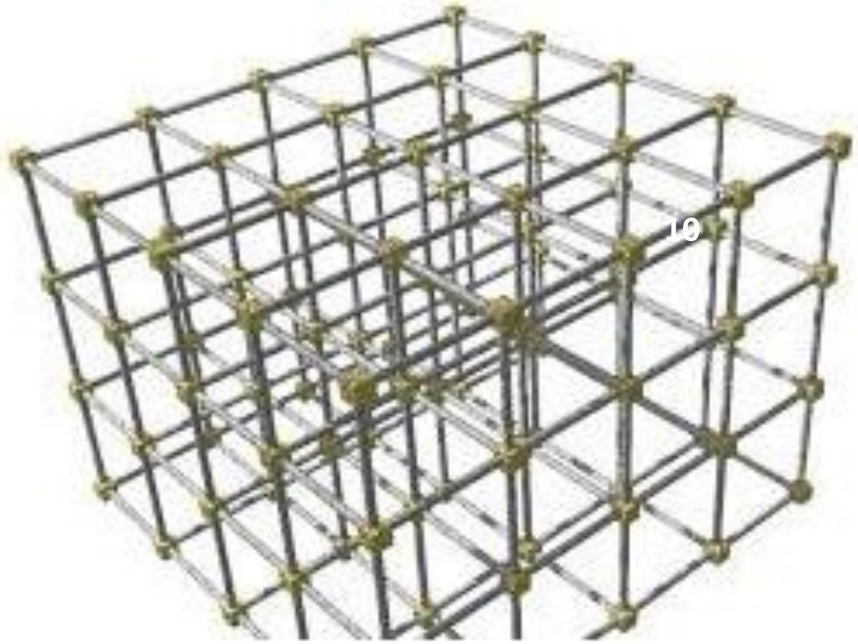
“Keunggulan Kompetitif, Bisnis Baru”

Apa dan Mengapa Keselarasan Strategi Antara Bisnis dan Teknologi Informasi (TI)?

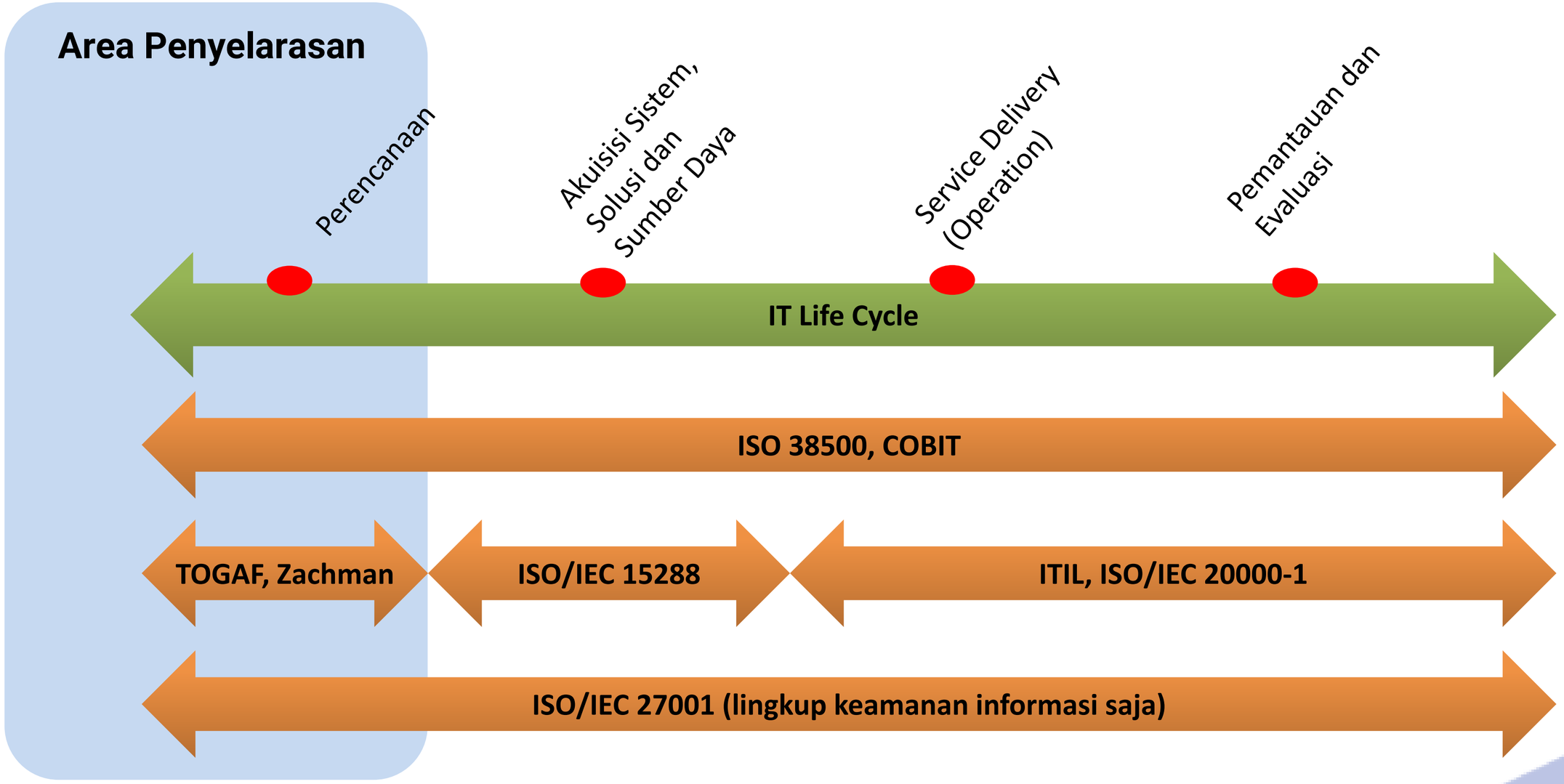
- Keselarasan strategi adalah **konsep yang menekankan pentingnya menyelaraskan strategi TI dengan strategi bisnis secara keseluruhan**.
- Keselarasan strategi **bertujuan untuk memastikan bahwa penggunaan TI memberikan kontribusi maksimal terhadap pencapaian tujuan dan nilai bisnis.**

Mengapa Kita Perlu Menerapkan “Best Practice Framework” untuk Keselarasan?

- Karena terlalu banyak *effort* untuk bisa memikirkan bagaimana metodolgi yang paling tepat untuk mencipatkan keselarasan TI dengan Bisnis.
- Karena kita perlu sharing knowledge dan pengalaman
- Karena kita perlu pengakuan (*recognizing*)
- Karena... (banyak hal)



Beberapa IT Best Practice Framework



Bagian II
Mengenal COBIT 2019

COBIT

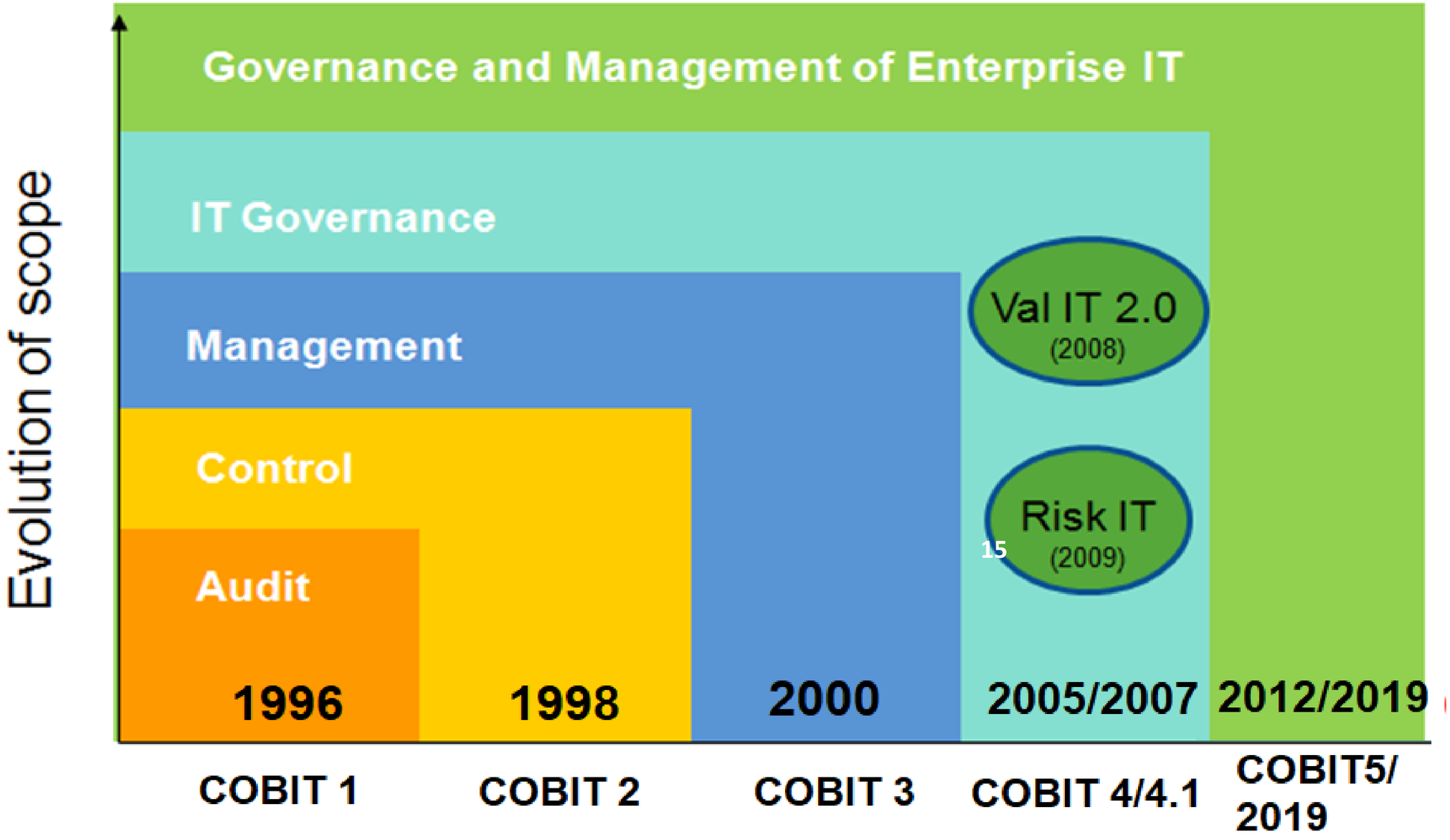
- **COBIT** (Control Objectives for Information and related Technology), merupakan ***Enterprise Governance of Information and Technology (EGIT) Framework*** terbitan ISACA (Information Systems Audit and Control Association), yang menekankan kepada **terciptanya keselarasan dengan kebutuhan bisnis** suatu organisasi serta memberikan **optimasi antara benefit dan risiko** dengan suatu pendekatan yang **holistik**.

- **COBIT** mencakup *governance* (arah/*direct*) dan *manage* (pengelolaan) terkait Teknologi dan Informasi di perusahaan/organisasi.

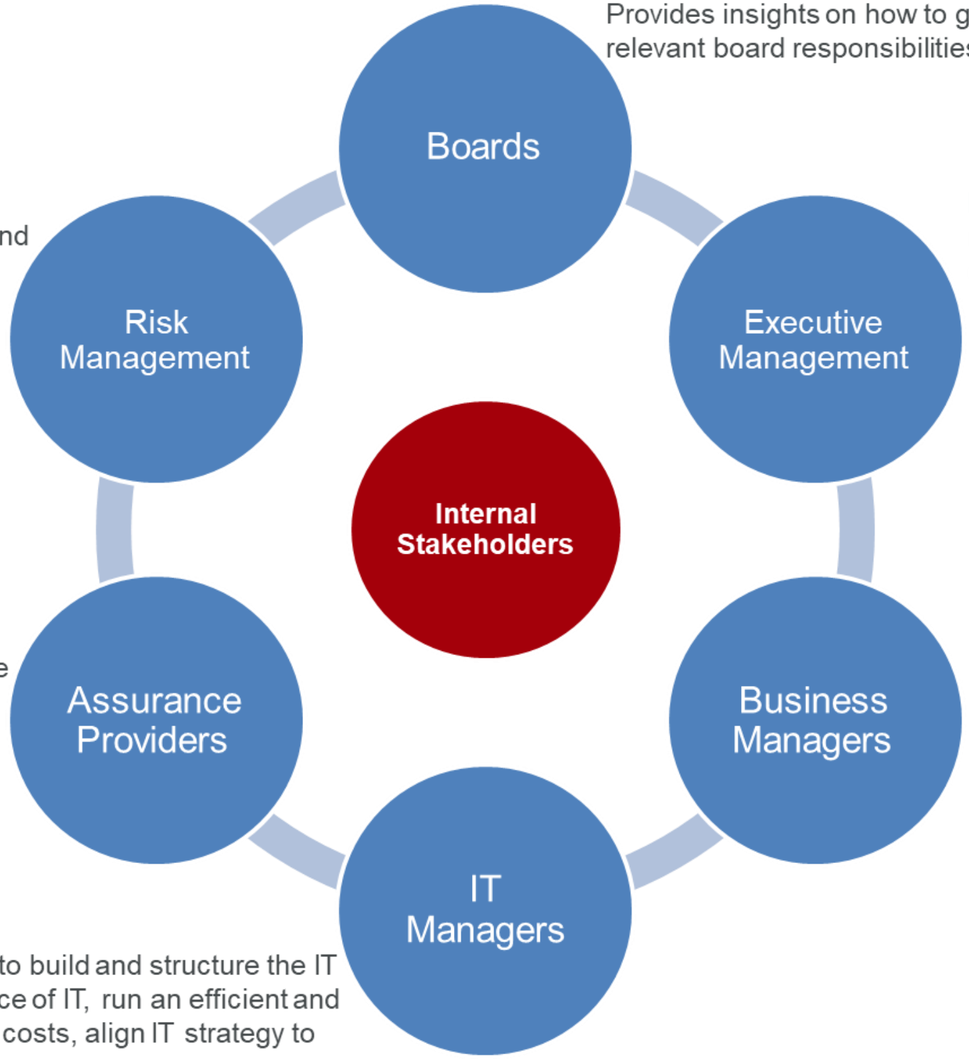
Perbedaan Antara IT dengan I&T (Menurut COBIT 2019)

- **Teknologi Informasi (TI atau *IT*)** mengacu kepada **pengelolaan teknologi terkait dengan informasi**, biasanya menjadi "urusan" fungsi tertentu di perusahaan (**cakupan Divisi TIK, Departement TI, dsb.**)
- **Teknologi dan Informasi (T&I atau dalam Bahasa Inggrisnya *I&T*)** mengacu kepada **pengelolaan teknologi** (apapun itu, baik terkait dengan informasi, operasional, dan sebagainya) serta **pengelolaan informasi** (baik terkait dengan teknologi maupun tata kelola/proses bisnisnya) dalam **cakupan *enterprise* (perusahaan/organisasi)**.

Sejarah COBIT



Stakeholder EGIT - Internal



Provides insights on how to get value from the use of I&T and explains relevant board responsibilities

Provides guidance on how to organize and monitor performance of I&T across the enterprise

Helps to understand how to obtain the I&T solutions enterprises require and how best to exploit new technology for strategic opportunities

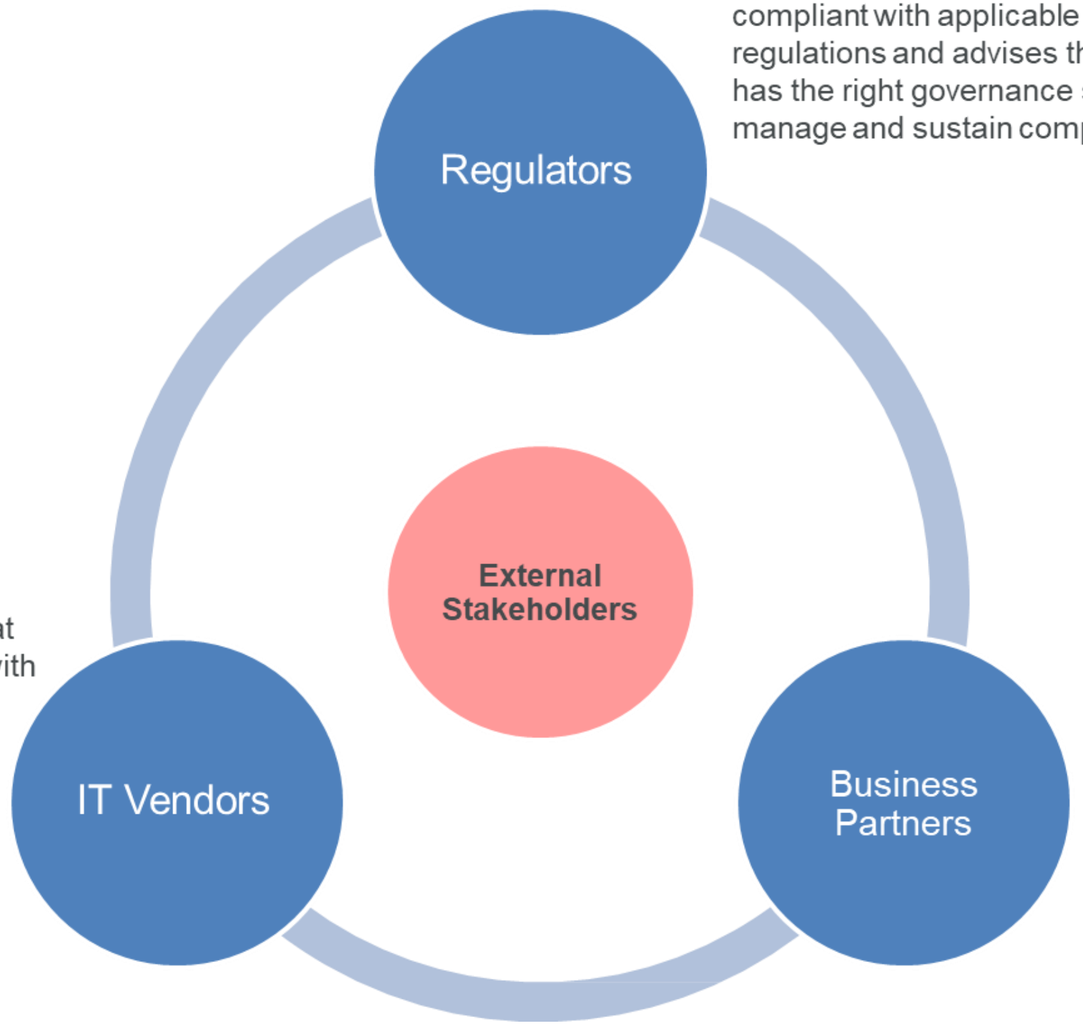
Provides guidance on how best to build and structure the IT department, manage performance of IT, run an efficient and effective IT operation, control IT costs, align IT strategy to business priorities, etc.

Helps manage dependencies on external service providers, provides assurance over IT, and ensures the existence of an effective and efficient system of internal controls

Helps to ensure the identification and management of all IT-related risk

Stakeholder EGIT - External

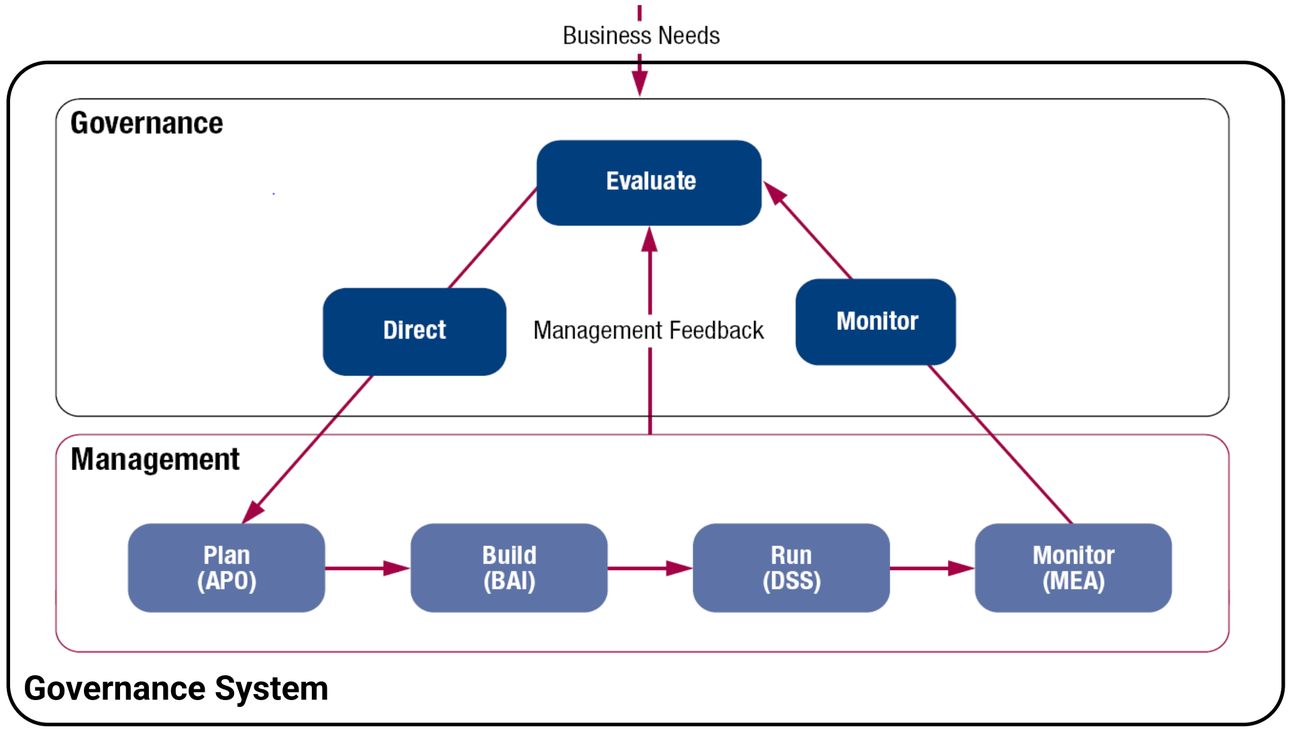
Determines whether the enterprise is compliant with applicable rules and regulations and advises that the enterprise has the right governance system in place to manage and sustain compliance



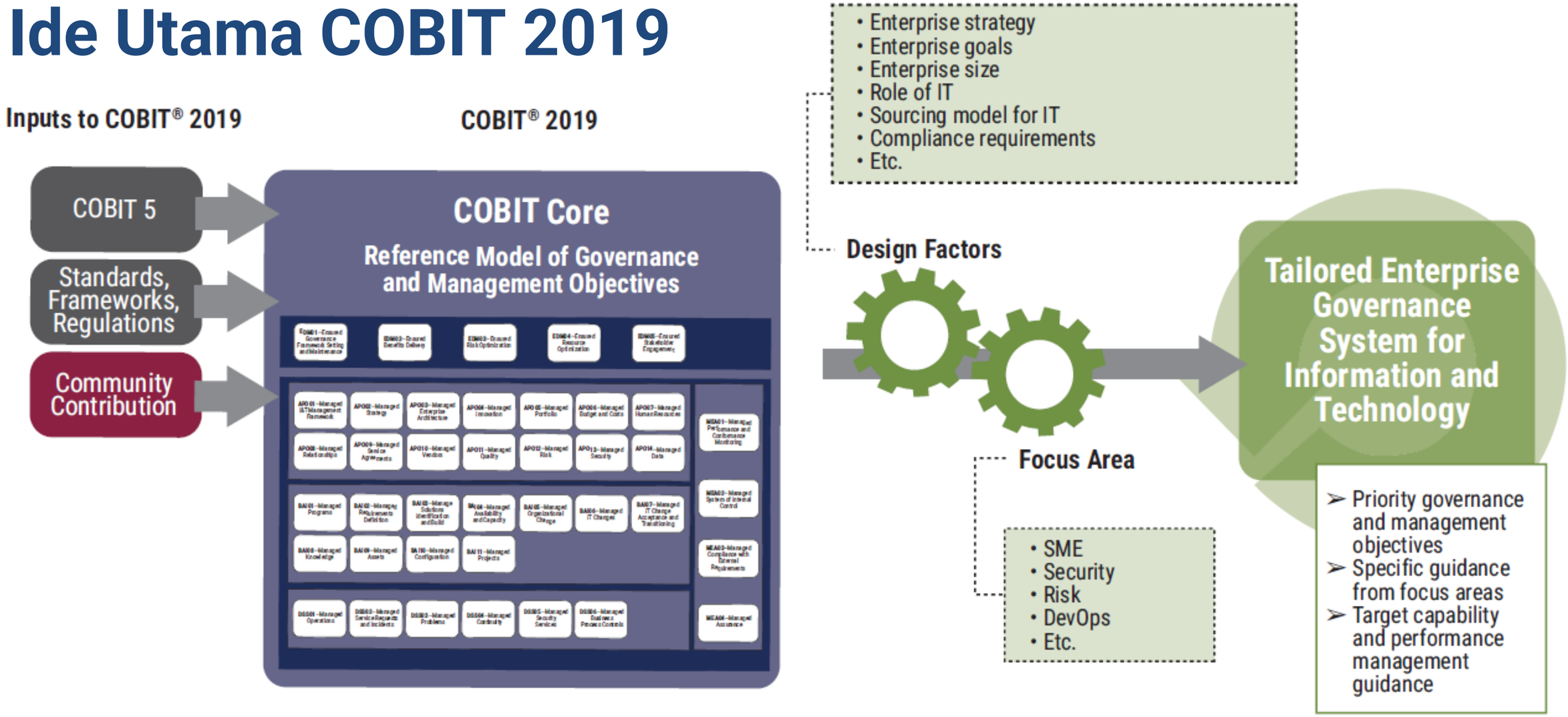
IT vendor's operations must establish that they are secure, reliable and compliant with applicable rules and regulations

Confirm that a business partner's operations are secure, reliable and compliant with applicable rules and regulations

Governance System Beserta Komponennya

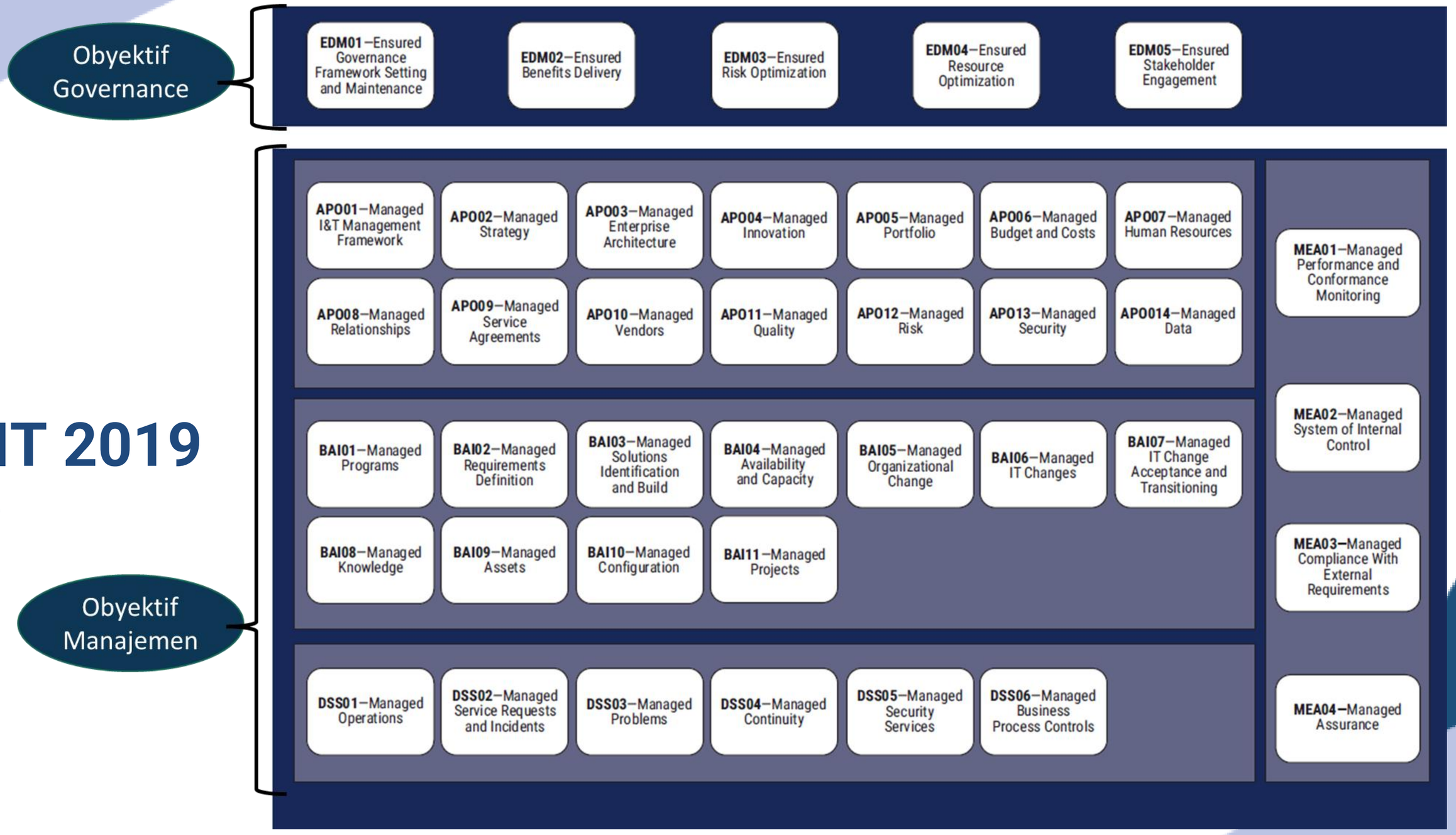


Ide Utama COBIT 2019



Baca: Sistem Tata Kelola T&I Perusahaan dirancang berbasiskan COBIT Core yang dikustomisasi melalui pertimbangan *design factor* dan *focus area*.

COBIT 2019 Core

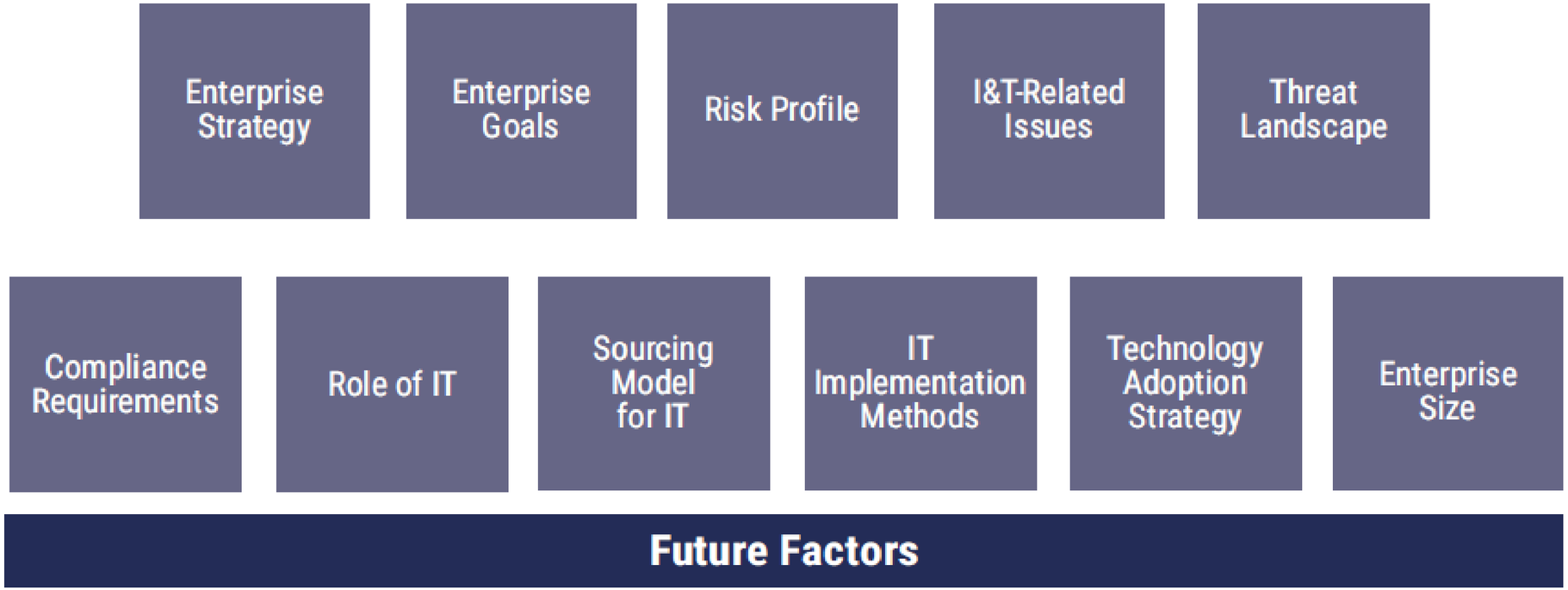


COBIT 2019 Design Factor

Design Factor adalah faktor yang:

- Mempengaruhi desain sistem tata kelola perusahaan
- Merupakan kunci sukes dalam menentukan "*fit for purpose*" I&T

Design Factor mencakup:



COBIT 2019 Focus Area

- *Focus Area* merupakan konsep yang diperkenalkan untuk **memberikan fleksibilitas dalam menerapkan prinsip-prinsip COBIT ke berbagai kebutuhan dan prioritas bisnis**.
- ISACA sudah menerbitkan beberapa (dan akan terus dikembangkan) panduan spesifik untuk penerapan COBIT 2019 per *focus area*.
- Beberapa *Focus Area* yang menjadi perhatian ISACA:
  - ✓ **Digital Transformation:** Fokus pada bagaimana organisasi dapat mengelola dan memanfaatkan teknologi digital untuk mendukung transformasi bisnis dan meningkatkan nilai.
  - ✓ **Cybersecurity:** Fokus pada pengelolaan risiko keamanan informasi, perlindungan aset informasi, dan pemenuhan kepatuhan terhadap regulasi keamanan.
  - ✓ **Cloud Computing:** Fokus pada tata kelola dan manajemen layanan cloud, termasuk strategi adopsi, pengelolaan risiko, dan pemantauan kinerja.

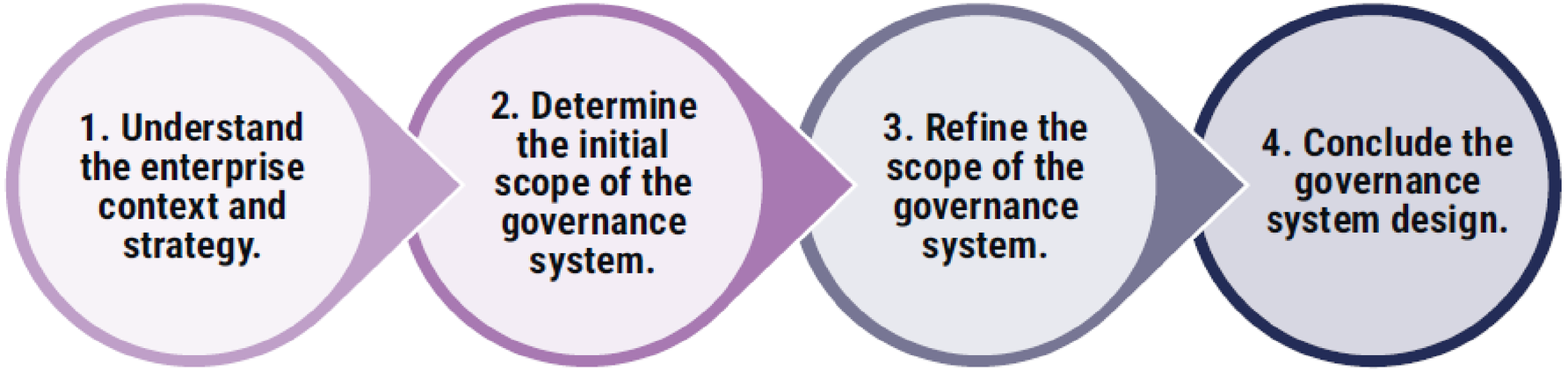
COBIT 2019 Focus Area (2)

- ✓ **DevOps:** Fokus pada integrasi dan otomatisasi antara tim pengembangan dan operasi untuk mempercepat pengiriman perangkat lunak dan meningkatkan kualitas.
- ✓ **Risk Management:** Fokus pada identifikasi, evaluasi, dan mitigasi risiko yang terkait dengan TI dan bisnis secara keseluruhan.
- ✓ **Innovation:** Fokus pada pengelolaan inovasi dan penerapan teknologi baru untuk mendukung tujuan strategis organisasi.
- ✓ **SME (Small and Medium Enterprises):** Fokus pada penerapan prinsip COBIT yang disesuaikan dengan kebutuhan dan sumber daya yang tersedia di perusahaan kecil dan menengah.

Bagian III

Merancang Keselarasan Strategi TI dengan Strategi Bisnis Menggunakan Pendekatan COBIT 2019

Tahapan Perancangan Tailored EGIT Menurut COBIT 2019 untuk Mengoptimalkan Keselarasan



- 1.1 Understand enterprise strategy.
- 1.2 Understand enterprise goals.
- 1.3 Understand the risk profile.
- 1.4 Understand current I&T-related issues.

- 2.1 Consider enterprise strategy.
- 2.2 Consider enterprise goals and apply the COBIT goals cascade.
- 2.3 Consider the risk profile of the enterprise.
- 2.4 Consider current I&T-related issues.

- 3.1 Consider the threat landscape.
- 3.2 Consider compliance requirements.
- 3.3 Consider the role of IT.
- 3.4 Consider the sourcing model.
- 3.5 Consider IT implementation methods.
- 3.6 Consider the IT adoption strategy.
- 3.7 Consider enterprise size.

- 4.1 Resolve inherent priority conflicts.
- 4.2 Conclude the governance system design.

Step 1.1 & 2.1: Understand The Enterprise Strategy

Perusahaan kita cenderung termasuk ke Strategy Archetype apakah?

Enterprise Strategy Design Factor	
Strategy Archetype	**Explanation**
Growth/Acquisition	The enterprise has a focus on growing (revenues)[2]
Innovation/Differentiation	The enterprise has a focus on offering different and/or innovative products and services to their clients[3]
Cost Leadership	The enterprise has a focus on short-term cost minimization[4]
Client Service/Stability	The enterprise has a focus on providing a stable and client-oriented service.[5]

Step 1.2 & 2.2: Understand The Enterprise Goal

Bagaimana goal Perusahaan kita kalau kita petakan ke dalam dimenasi Balanced Scorecard (BSC) dalam Perpsektif Design Factor Berikut?

Enterprise Goals Design Factor		
Reference	**Balanced Scorecard (BSC) Dimension**	**Enterprise Goal**
EG01	Financial	Portfolio of competitive products and services
EG02	Financial	Managed business risk
EG03	Financial	Compliance with external laws and regulations
EG04	Financial	Quality of financial information
EG05	Customer	Customer-oriented service culture
EG06	Customer	Business service continuity and availability
EG07	Customer	Quality of management information
EG08	Internal	Optimization of internal business process functionality
EG09	Internal	Optimization of business process costs
EG10	Internal	Staff skills, motivation and productivity
EG11	Internal	Compliance with internal policies
EG12	Growth	Managed digital transformation programs
EG13	Growth	Product and business innovation

Step 1.3 & 2.3: Understand The Risk Profile (1)

Bagaimana profil risiko kita jika kita petakan ke katalog profil risiko berdasarkan Design Factor berikut ini?

Risk Profile Design Factor (IT Risk Categories)		
Reference	**Risk Category**	**Example Risk Scenarios**
1	IT-investment decision making, portfolio definition and maintenance	A. Programs selected for implementation misaligned with corporate strategy and priorities B. Failure of IT-related Investments to support digital strategy of the enterprise C. Selection of wrong software (in terms of cost, performance, features, compatibility, redundancy, etc.) for acquisition and implementation D. Selection of wrong infrastructure (in terms of cost, performance, features, compatibility, etc.) for implementation E. Duplication or important overlaps between different investment initiatives F. Long-term incompatibility between new investment programs and enterprise architecture G. Misallocation, inefficient management and/or competition for resources without alignment to business priorities
2	Program and projects lifecycle management	A. Failure of senior management to terminate failing projects (due to cost explosion, excessive delays, scope creep, changed business priorities) B. Budget overruns for I&T projects C. Lack of quality of I&T projects D. Late delivery of I&T projects E. Failure of third-party outsourcers to deliver projects as per contractual agreements (any combination of exceeded budgets, quality problems, missing functionality, late delivery)
3	IT cost and oversight	A. Extensive dependency on, and use of, user-created, user-defined, user-maintained applications and *ad hoc* solutions B. Excess cost and/or ineffectiveness of I&T-related purchases outside of the I&T procurement process C. Inadequate requirements leading to ineffective Service Level Agreements (SLAs) D. Lack of funds for I&T related investments
4	IT expertise, skills and behavior	A. Lack or mismatch of IT-related skills within IT (e.g., due to new technologies or working methods) B. Lack of business understanding by IT staff that affects service delivery/project quality C. Inability to recruit and retain IT staff D. Recruitment of unsuitable profiles because of lack of due diligence in the recruitment process E. Lack of I&T training F. Overreliance for I&T services on key staff

Step 1.3 & 2.3: Understand The Risk Profile (2)

Bagaimana profil risiko kita jika kita petakan ke katalog profil risiko berdasarkan Design Factor berikut ini?

5	Enterprise/IT architecture	A. Complex, inflexible enterprise architecture (EA), obstructing further evolution and expansion, and leading to missed business opportunities B. Failure to timely adopt and exploit new infrastructure or abandon obsolete infrastructure C. Failure to timely adopt and exploit new software (functionality, optimization, etc.) or to abandon obsolete applications D. Undocumented EA leading to inefficiencies and duplications E. Excessive number of exceptions on enterprise architecture standards
6	IT operational infrastructure incidents	A. Accidental damaging of IT equipment B. Errors by IT staff (during backup, during upgrades of systems, during maintenance of systems, etc.) C. Incorrect information input by IT staff or system users D. Destruction of data center (sabotage, etc.) by staff E. Theft of device with sensitive data F. Theft of a key infrastructure component G. Erroneous configuration of hardware components H. Intentional tampering with hardware (security devices, etc.) I. Abuse of access rights from prior roles to access IT infrastructure J. Loss of backup media or backups not checked for effectiveness K. Loss of data by cloud provider L. Operational-service interruption by cloud providers
7	Unauthorized actions	A. Tampering with software B. Intentional modification or manipulation of software leading to incorrect data C. Intentional modification or manipulation of software leading to fraudulent actions D. Unintentional modification of software leading to inaccurate results E. Unintentional configuration and change-management errors
8	Software adoption/ usage problems	A. Nonadoption of new application software by users B. Inefficient use of new software by users

Step 1.3 & 2.3: Understand The Risk Profile (3)

Bagaimana profil risiko kita jika kita petakan ke katalog profil risiko berdasarkan Design Factor berikut ini?

9	Hardware incidents	A. System instability in wake of installing new infrastructure, leading to operational incidents (e.g., BYOD program) B. Inability of systems to handle transaction volumes when user volumes increase C. Inability of systems to handle load when new applications or initiatives are deployed D. Utilities failure (telecom, electricity) E. Hardware failure due to overheating and/or other environmental conditions like humidity F. Damaging of hardware components leading to destruction of data by internal staff G. Loss/disclosure of portable media containing sensitive data (CD, USB-drives, portable disks, etc.) H. Extended resolution time or support delays in case of hardware incidents
10	Software failures	A. Inability to use the software to realize desired outcomes (e.g., failure to make required business model or organizational changes) B. Implementation of immature software (early adopters, bugs, etc.) C. Operational glitches when new software is made operational D. Regular software malfunctioning of critical application software E. Obsolete application software (outdated, poorly documented, expensive to maintain, difficult to extend, not integrated in current architecture, etc.) F. Inability to revert back to former versions in case of operational issues with a new version G. Software-induced corrupted data(base) leading to inaccessible data
11	Logical attacks (hacking, malware, etc.)	A. Unauthorized (internal) users trying to break into systems B. Service interruption due to denial-of-service (DoS) attack C. Website defacement D. Malware attack E. Industrial espionage F. Hacktivism G. Disgruntled employee implements a time bomb which leads to data loss H. Company data stolen through unauthorized access gained by a phishing attack I. Foreign government attacks on critical systems

Step 1.3 & 2.3: Understand The Risk Profile (4)

Bagaimana profil risiko kita jika kita petakan ke katalog profil risiko berdasarkan Design Factor berikut ini?

12	Third-party/supplier incidents	A. Inadequate performance of outsourcer in large-scale, long-term outsourcing arrangement (e.g., through lack of supplier due diligence regarding financial viability, delivery capability and sustainability of supplier's service) B. Accepting unreasonable terms of business from IT suppliers C. Inadequate support and services delivered by vendors, not in line with SLA D. Noncompliance with software license agreements (use and/or distribution of unlicensed software) E. Inability to transfer to alternative suppliers due to overreliance or overdependence on current supplier F. Purchase of IT services (especially cloud services) by the business without consultation /involvement of IT, resulting in inability to integrate the service with in-house services. G. Inadequate or unenforced SLA to obtain agreed services and penalties in case of noncompliance
13	Noncompliance	A. Noncompliance with national or international regulations (e.g., privacy, accounting, manufacturing, environmental, etc.) B. Lack of awareness of potential regulatory changes that may have a business impact C. Operational obstacles caused by regulations D. Failure to comply with internal procedures
14	Geopolitical issues	A. Lack of access due to disruptive incident in other premises B. Government interference and national policies impacting the business C. Targeted action from government-sponsored groups or agencies
15	Industrial action	A. Facilities and building inaccessible because of labor union strike B. Third-party providers unable to provide services because of strike C. Key staff unavailable through industrial action (e.g., transportation or utilities strike)

Step 1.3 & 2.3: Understand The Risk Profile (5)

Bagaimana profil risiko kita jika kita petakan ke katalog profil risiko berdasarkan Design Factor berikut ini?

16	Acts of nature	A. Earthquake destroying or damaging important IT infrastructure B. Tsunami destroying critical premises C. Major storms and tropical cyclone or tornado damaging critical infrastructure D. Major wildfire E. Flooding F. Rising water table leaving critical location unusable G. Rising temperature rendering critical locations uneconomical to operate
17	Technology-based innovation	A. Failure to identify new and important technology trends B. Failure to appreciate the value and potential of new technologies C. Failure to adopt and exploit new technologies in a timely manner (functionality, process optimization, etc.) D. Failure to provide technology support new business models
18	Environmental	A. Environmentally unfriendly equipment (e.g., power consumption, packaging)
19	Data and information management	A. Discovery of sensitive information by unauthorized persons due to inefficient retaining/archiving/disposing of information B. Intentional illicit or malicious modification of data C. Unauthorized disclosure of sensitive information through email or social media D. Loss of IP and/or leakage of competitive information

Step 2.4: Understand The Current I&T Related Issues

Apa saja isu-isu terkiat I&T yang dihadapi oleh Perusahaan dalam Perspektif Design Factor?

I&T-Related Issues Design Factor	
Reference	**Description**
A	Frustration between different IT entities across the organization because of a perception of low contribution to business value
B	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value
C	Significant IT related incidents, such as data loss, security breaches, project failure, application errors, etc. linked to IT
D	Service delivery problems by the IT outsourcer(s)
E	Failures to meet IT related regulatory or contractual requirements
F	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
G	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets
H	Duplications or overlaps between various initiatives or other forms of wasting resources
I	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction
J	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget
K	Reluctance by board members, executives or senior management to engage with IT, or lack of committed business sponsors for IT
L	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions
M	Excessively high cost of IT
N	Obstructed or failed implementations of new initiatives or innovations caused by the current IT architecture and system
O	Gap between business and technical knowledge which leads to business users and IT and/or technology specialists speaking different languages
P	Regular issues with data quality and integration of data across various sources
Q	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation
R	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department [8]
S	Ignorance and/or noncompliance with security and privacy regulations
T	Inability to exploit new technologies or to innovate using I&T

Step 3.1: Threat Landscape

Bagaimanakah gambaran ancaman yang sedang dan akan berdampak pada Perusahaan?

Threat Landscape Design Factor	
Threat Landscape	**Explanation**
Normal	The enterprise is operating under what are considered normal threat levels
High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.

Step 3.2: Consider Compliance Requirement

Bagaimanakah Compliance Requirement terhadap Perusahaan?

Compliance Requirements Design Factor	
Regulatory Environment	**Explanation**
Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.
Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.
High compliance requirements	The enterprise is subject to higher than average compliance requirements, most often related to industry sector or geopolitical conditions.

Step 3.3: Consider Role of IT

Bagaimanakah Peran IT di Perusahaan?

Role of IT Design Factor	
Role of IT[9]	**Explanation**
Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.
Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.
Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency of IT for the current running and continuity of the business processes and services.
Strategic	IT is critical for both running and innovating the organization's business processes and services.

Step 3.4: Consider Sourcing Model

Bagaimanakah Sourcing Model terhadap IT di Perusahaan?

Sourcing Model for IT Design Factor	
Sourcing Model	**Explanation**
Outsourcing	The enterprise calls upon the services of a third party to provide IT services.
Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.
Insourced	The enterprise provides for their own IT staff and services.
Hybrid	A mixed model is applied, combining the three models above in varying degrees.

Step 3.5: Consider IT Implementation Method

Bagaimanakah Metode Implementasi IT di Perusahaan?

IT Implementation Methods Design Factor	
IT Implementation Method	**Explanation**
Agile	The enterprise uses Agile development working methods for its software development.
DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.
Traditional	The enterprise uses a more classic approach towards software development (waterfall) and separates software development and operations.
Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as "bimodal IT."

Step 3.6: Consider Technology Adoption Strategy

Bagaimanakah adopsi teknologi yang berlaku di Perusahaan?

Technology Adoption Strategy Design Factor	
Technology Adoption Strategy	**Explanation**
First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.
Follower	The enterprise typically waits for new technology to become mainstream and proven before adopting them.
Slow adopter	The enterprise is very late with their adoption of new technologies.

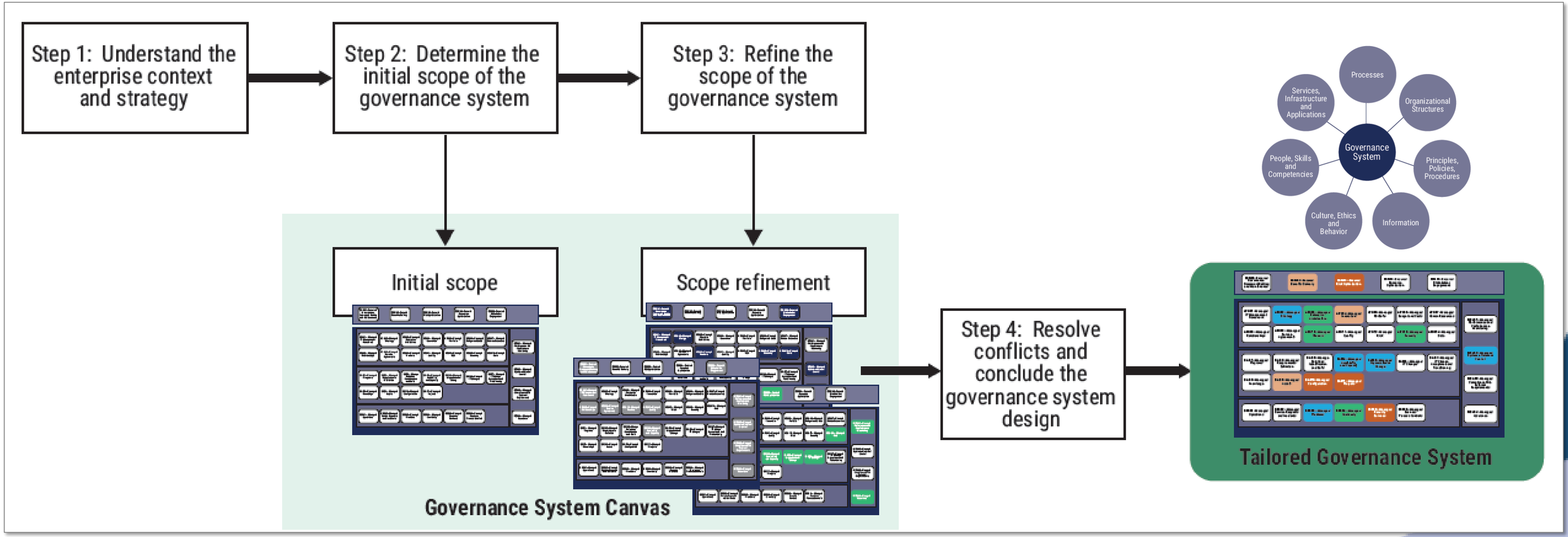
Step 3.7: Consider Enterprise Size

Bagaimanakah skala Perusahaannya?

Enterprise Size Design Factor	
Enterprise Size	**Explanation**
Large enterprise (default)	Enterprises with more than 250 full-time employees (FTEs)
Small and medium enterprise	Enterprise with 50 to 250 FTEs

Step 4.1 & 4.2: Resolve Conflicts & Conclude

Kesimpulan: COBIT 2019 Core objective beserta komponen yang mana yang akan diimplementasikan dalam "*Tailored Governance System*"?



Bagian IV
Kesimpulan

Kesimpulan

- Perusahaan perlu memastikan adanya keselarasan antara Strategi Perusahaan & Strategi TI.
- Banyak kerangka kerja yang digunakan untuk memastikan keselarasan antara Strategi Perusahaan & Strategi TI.
- COBIT 2019 adalah salah satu kerangka kerja tata Kelola Teknologi dan Informasi yang memiliki pendekatan yang sistematis untuk membangun keselarasan antara Strategi Perusahaan & Strategi TI.

About Us

ISO CENTER INDONESIA adalah penyedia layanan terkait ISO dan Sistem Manajemen yang komprehensif. Kami adalah The Ultimate ISO and Management System Resources yang siap meningkatkan kinerja organisasi Anda melalui penyediaan informasi, pelatihan, implementasi, dan asesmen standar internasional berbasis ISO dan sistem manajemen yang efektif, efisien, out of the box, dan menggunakan metode terkini yang di-enable oleh teknologi dan AI.Jangan lupa untuk selalu kunjungi situs kami dan mengakses tautan Articles yang memuat kajian-kajian terkini kami dan Download yang berisi video-video pembalajaran, e-book hasil riset kami, dan alat-alat bantu yang berupa kertas-kertas kerja dan template yang selau kami kinikan.

Semua itu kami persembahkan untuk Anda!

Thank You!

ISO Center Indonesia (Jakarta)

Permata Kuningan Building 17th Floor, HR Rasuna Said. Kuningan Mulia, Menteng Atas, Setia Budi, South Jakarta City, Jakarta 12920

East Office (Surabaya)

AMG Tower Lantai 17, Jl. Raya Dukuh Menanggal No 1A, East Java, Gayungan Surabaya, Indonesia 60234

Contact Us :

Website : https://isoindonesiacenter.com/
Email : admin@isoindonesiacenter.com
Telepon : +62 813-184-5942 (Sinthia - WhatsApp/Call)
+62 895-2956-5008 (Louqman – WhatsApp/Call)
+62 89-6551-88175 (Ardi - WhatsApp/Call)