PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS 17 AGUSTUS 1945 SURABAYA

SEMESTER
GASAL
2023/2024

Tata Kelola TI dan Manajemen Risiko

Pertemuan 3 - 4

14620403 – AUDIT TEKNOLOGI INFORMASI

INTAN DZIKRIA, PH.D.

LEARNING OUTCOMES

SubCPMK3 - Mengenali prinsip utama tata kelola TI dan memahami penerapan kerangka kerja kontrol dalam mengelola risiko TI.

SubCOMK4 - Mengidentifikasi berbagai jenis risiko TI dan menerapkan teknik penilaian risiko untuk memprioritaskan dan mengelolanya

INDIKATOR CAPAIAN :

3.1. Menjelaskan prinsip utama tata kelola TI dan keselarasannya dengan tujuan bisnis.

3.2. Menjelaskan pentingnya kerangka kontrol seperti COBIT dalam mengelola risiko TI.

4.1. Mengidentifikasi berbagai jenis risiko TI dan potensi dampaknya.

4.2. Menerapkan teknik penilaian risiko untuk mengevaluasi dan memprioritaskan risiko TI.

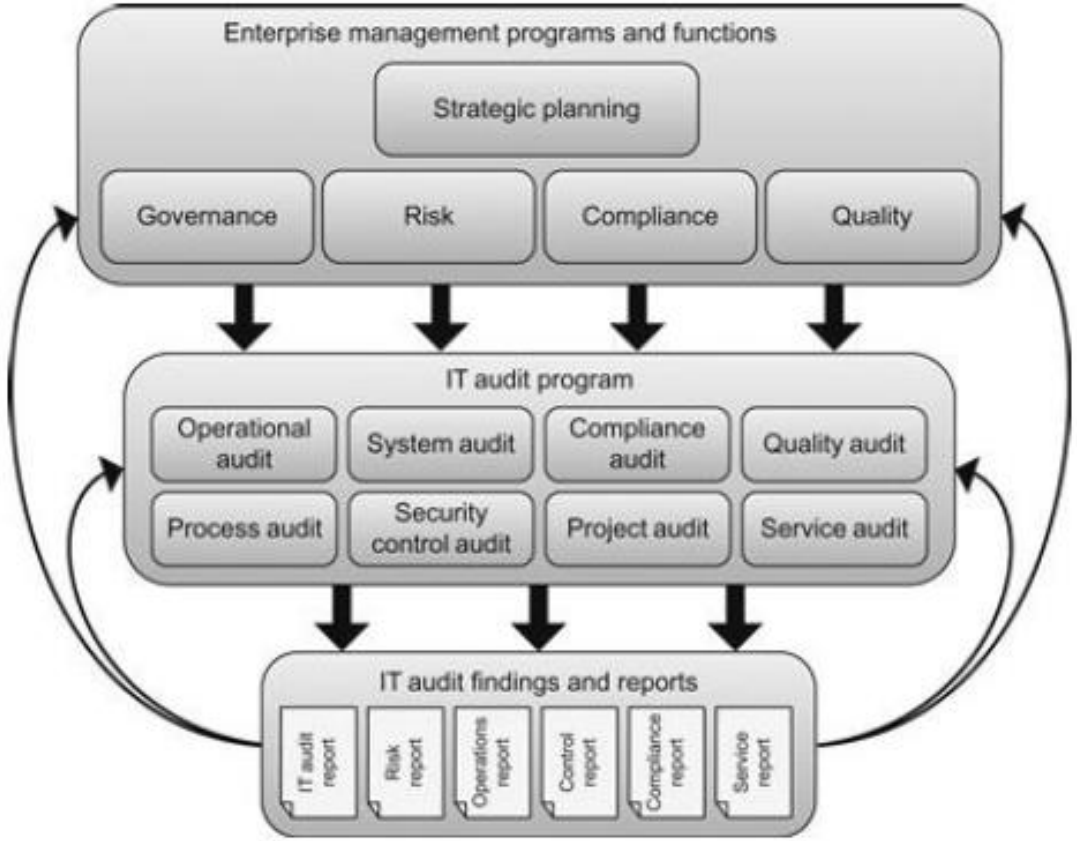
OUTLINES

1. *IT Governance*
2. *Risk Management*
3. *Legal and Regulatory Compliance*
4. *Quality Management and Assurance*
5. *Information Security Management*

Dengan pengecualian organisasi yang tunduk pada peraturan atau kebijakan eksternal yang mengharuskan mereka menjalankan fungsi audit internal atau melakukan audit teknologi informasi (TI), keputusan untuk menetapkan kemampuan audit TI internal biasanya didorong oleh tujuan yang ditetapkan secara internal. Dorongan utama yang mendorong organisasi untuk menyiapkan dan mengoperasikan program audit TI adalah **kebutuhan untuk memberikan dukungan terhadap inisiatif atau program manajemen perusahaan yang bergantung pada TI.**

Gantz (2014)

IT Audit Activities



Aktivitas audit TI merupakan bagian integral dari beberapa fungsi utama manajemen perusahaan, yang secara kolektif berkontribusi terhadap cakupan program audit TI dan menerima masukan dari keluaran proses audit.

Gantz (2014)

1 IT Governance

TATA KELOLA TEKNOLOGI INFORMASI

DEFINITION OF GOVERNANCE

Konteks Bisnis - Governance

the set of policies, processes, and actions taken by management to define organizational strategy and operate the organization in a way intended to help realize its business goals and objectives

Serangkaian kebijakan, proses, dan tindakan yang diambil oleh manajemen untuk menentukan strategi organisasi dan mengoperasikan organisasi dengan cara yang dimaksudkan untuk membantu mewujudkan tujuan dan sasaran bisnisnya

Gantz (2014)

Konteks Teknologi – IT Governance

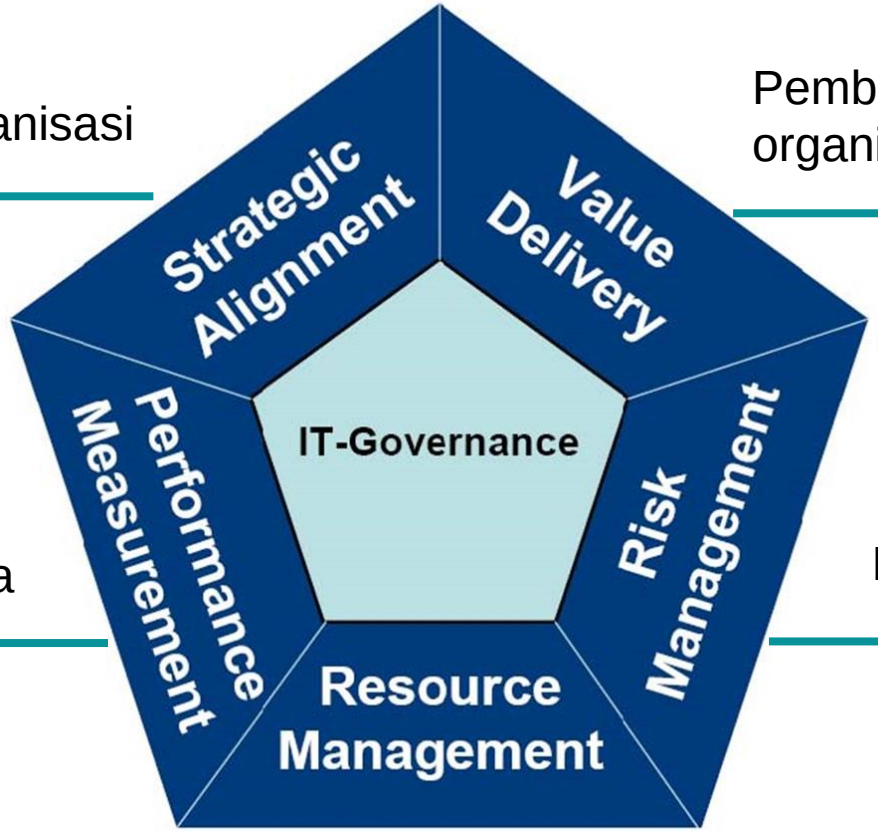
the structure and processes organizations use to try to ensure that their IT operations support the overall goals and objectives of the organization

Struktur dan proses yang digunakan organisasi untuk mencoba memastikan bahwa operasi TI mereka mendukung tujuan dan sasaran organisasi secara keseluruhan

SCOPE OF IT GOVERNANCE

Keselarasan Strategis Organisasi

Pemberian / Penambahan nilai pada organisasi



Penilaian Performa

Manajemen Risiko

Manajemen Sumber Daya

Gantz (2014)

Seperti yang diterapkan dalam praktiknya, tata kelola TI mencakup berbagai macam proses dan kontrol untuk aplikasi, sistem, jaringan, infrastruktur, personel, dan pusat data serta fasilitas lainnya, termasuk:

- Kebijakan terkait TI
- Prosedur operasional standar
- Rencana pengelolaan
- Pemantauan dan pengelolaan kinerja
- Fungsi pengawasan atau pengawasan
- Pengendalian TI dan pemantauan pengendalian
- Proses pengembangan sistem dan perangkat lunak
- Kegiatan operasi dan pemeliharaan.

Gantz (2014)

COBIT 5

Control Objectives for Information and Related Technology

ISO 38500

Corporate Governance Standard of Information Technology

Gantz (2014)

The Information Technology Infrastructure Library

ISO 2000 - Service Management

ISO 15504 – Software Development Processes

ISO 27000 – Risk Management

The Project Management Body of Knowledge (PMBOK)

Projects in Controlled Environments version 2 (PRINCE2)

Capability Maturity Model Integration

Gantz (2014)

Peran Audit TI dalam Tata Kelola

Penggunaan Framework dalam Tata Kelola

Organisasi tidak perlu mengikuti kerangka kerja (framework) yang ditetapkan secara formal untuk mempraktikkan tata kelola yang efektif.

Bagi organisasi yang melakukan hal tersebut, kerangka kerja serta standar dan prosedur yang terkait memberikan elemen dasar dasar audit TI yang digunakan di bidang yang dicakup oleh kerangka tata kelola.

Organisasi yang mengembangkan metodologi tata kelola mereka sendiri juga perlu menentukan serangkaian kriteria audit yang sesuai.

Organisasi juga perlu mendukung tata kelola dengan fungsi audit TI yang efektif yang memungkinkan mereka memvalidasi bahwa proses mereka berjalan sebagaimana mestinya; bahwa sistem mereka diterapkan, dikonfigurasi, dan dioperasikan dengan benar dan efektif; dan bahwa sumber daya yang mereka alokasikan untuk inisiatif TI mereka selaras dengan tujuan bisnis organisasi mereka.

Gantz (2014)

Peran Audit Teknologi Informasi

Kebijakan dan prosedur yang ditentukan oleh organisasi biasanya merupakan panduan yang dimaksudkan untuk memastikan bahwa TI digunakan secara efektif dan efisien dan bahwa tujuan kinerja yang ditetapkan tercapai.

Melakukan audit TI terhadap operasi internal adalah salah satu cara untuk memastikan bahwa proses dan aktivitas benar-benar dilaksanakan oleh organisasi sesuai dengan kebijakan dan prosedur dan untuk mengidentifikasi area ketidaksepakatan.

Jika suatu organisasi melacak biaya atau alokasi sumber daya TI lainnya dan menerapkan pengukuran kinerja yang konsisten, hasil audit TI dapat dikorelasikan dengan data biaya dan kinerja untuk memberikan beberapa wawasan tentang kontribusi operasi TI dalam mencapai tujuan bisnis dan hasil yang diinginkan.

Gantz (2014)

Peran Audit Teknologi Informasi

Selain memberikan informasi kepada manajemen tentang operasi TI, audit TI jenis ini juga dapat memberikan bukti untuk menunjukkan bahwa proses yang diterapkan organisasi menunjukkan tingkat kematangan atau sesuai dengan kriteria yang ditentukan secara eksternal seperti yang ada di CMMI atau Six Sigma, yang merupakan metodologi perbaikan teknologi informasi.

Audit TI dapat mengkonfirmasi pencapaian (atau kegagalan untuk mencapai) tujuan organisasi yang berkaitan dengan masing-masing fungsi

Gantz (2014)

2 Risk Management

MANAJEMEN RISIKO

Risiko vs Masalah

Masa Lalu | **Masa Kini** | **Masa Depan**

Keputusan/
Aktivitas

- ❖ Telah terjadi
- ❖ Akibat keputusan masa lalu

Masalah

Tindakan

Manajemen masalah/krisis/bencana

Keputusan/
Aktivitas

Tindakan

Manajemen masalah/
krisis

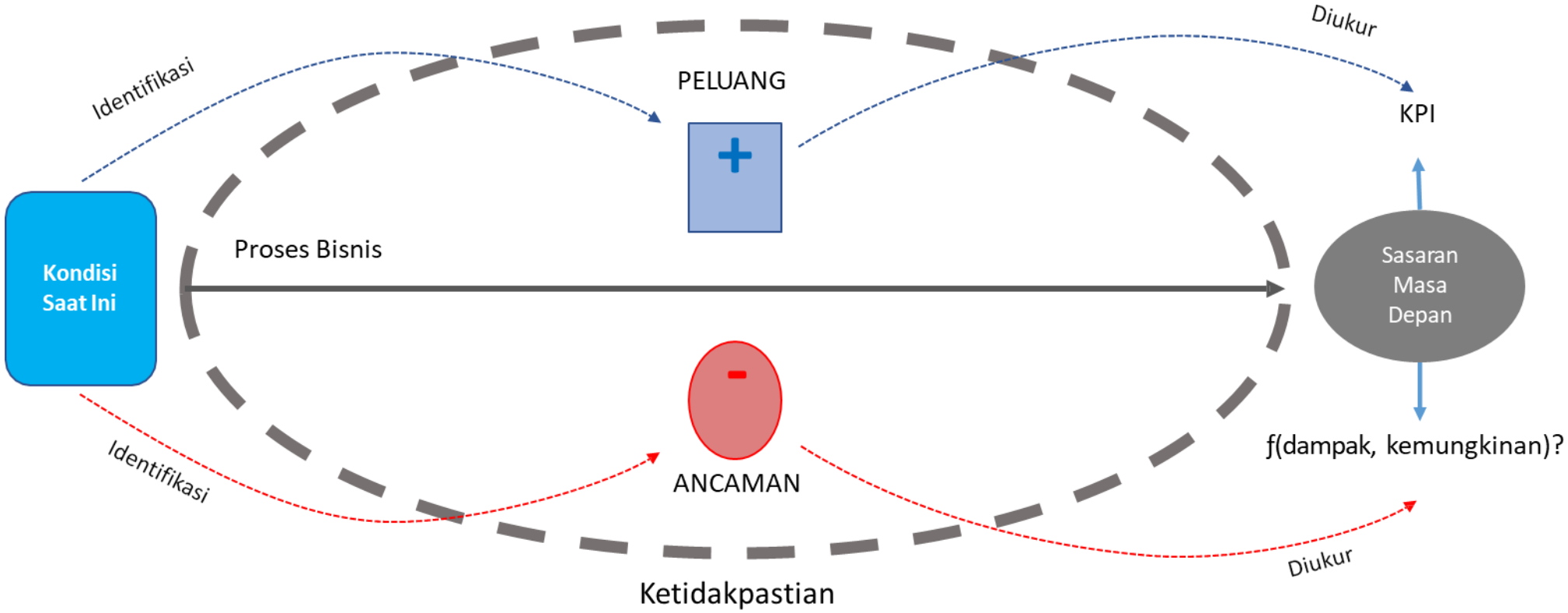
- ❖ Belum terjadi (potensi risiko)
- ❖ Akibat keputusan saat ini

Risiko

- Tidak ada kejutan
- Pencapaian tujuan

CRMS Indonesia (2023)

Keterkaitan antara Sasaran, Ketidakpastian, Risiko dan Peluang



CRMS Indonesia (2023)

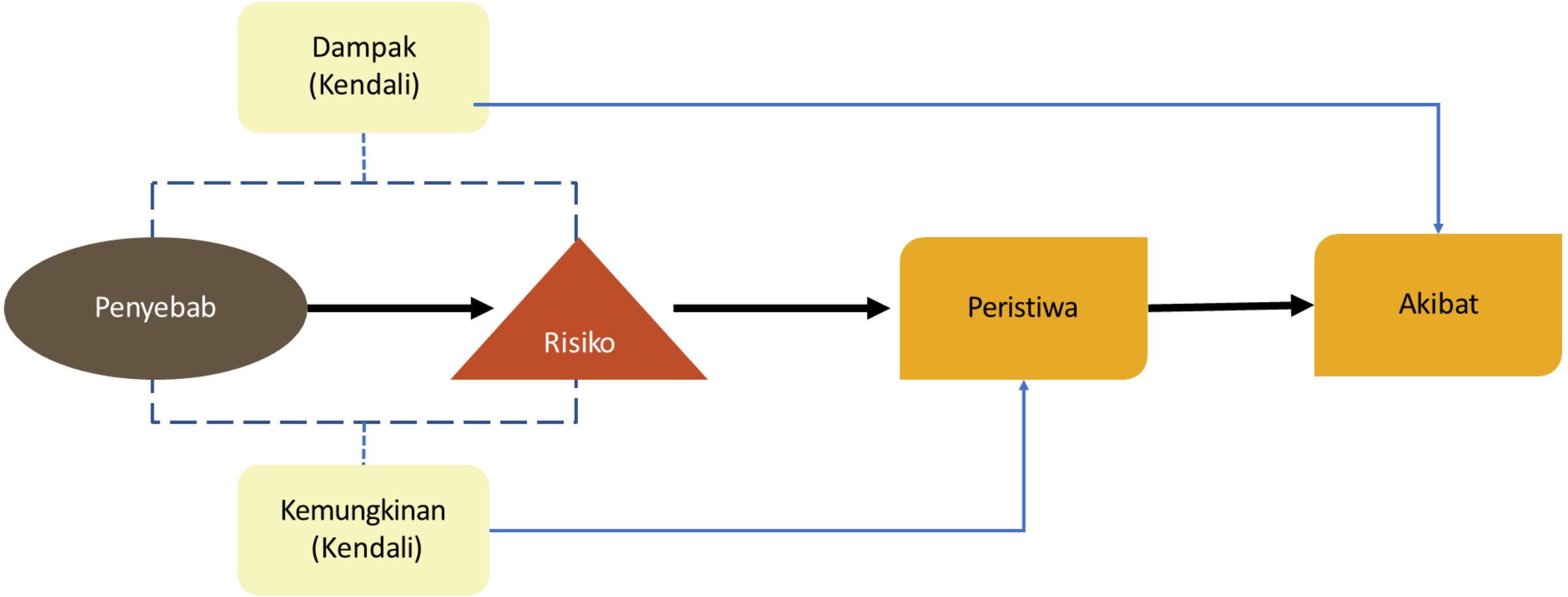
Definisi Risiko menurut SNI ISO 31000

= **Efek** dari **ketidakpastian** pada **sasaran**

(*Effect of uncertainty on objectives* – ISO 31000)

CRMS Indonesia (2023)

Definisi Risiko

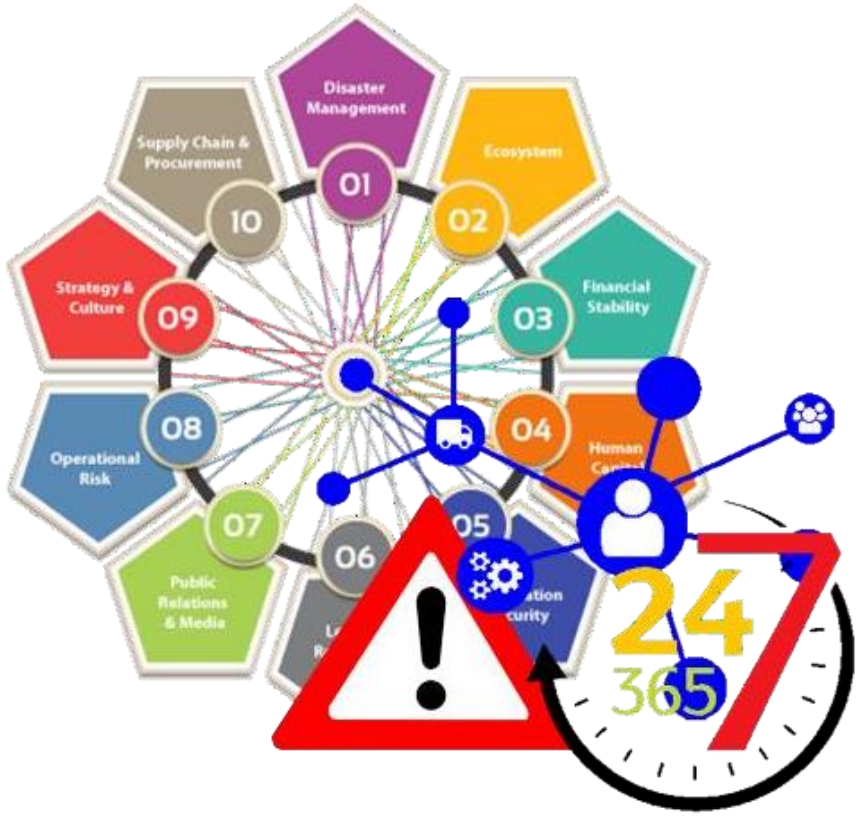


CRMS Indonesia (2023)

Definisi Manajemen Risiko menurut SNI ISO 31000

Manajemen Risiko adalah “aktivitas terkoordinasi untuk mengarahkan dan mengendalikan organisasi terkait risiko”

*Risk management is “*coordinated activities to direct and control an organization with regard to risk*”*



CRMS Indonesia (2023)

Definisi Pemilik Risiko menurut SNI ISO 31000

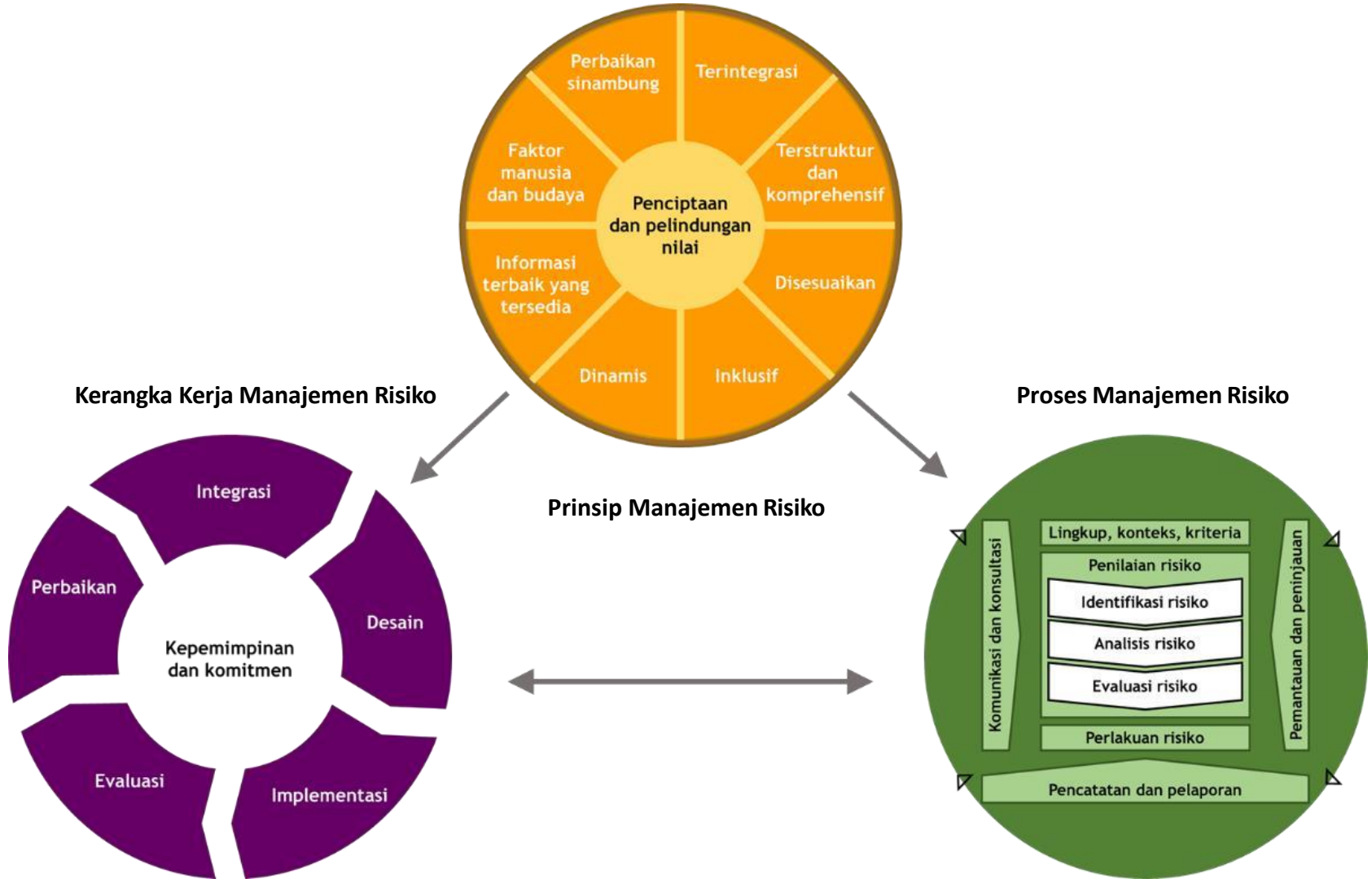
PEMILIK RISIKO = Orang atau entitas dengan **akuntabilitas** dan **wewenang** untuk mengelola risiko

(*Person or entity with the **accountability** and **authority** to manage risk – ISO 31000*)

CRMS Indonesia (2023)

CRMS Indonesia (2023)

Unsur Pengendalian Internal Menurut COSO



CRMS Indonesia (2023)

Unsur Pengendalian Internal Menurut COSO

Lingkungan Internal termasuk didalamnya: Organisasi, SDM, Kebijakan dan Prosedur

Penentuan Objek Pengendalian

Identifikasi Peristiwa

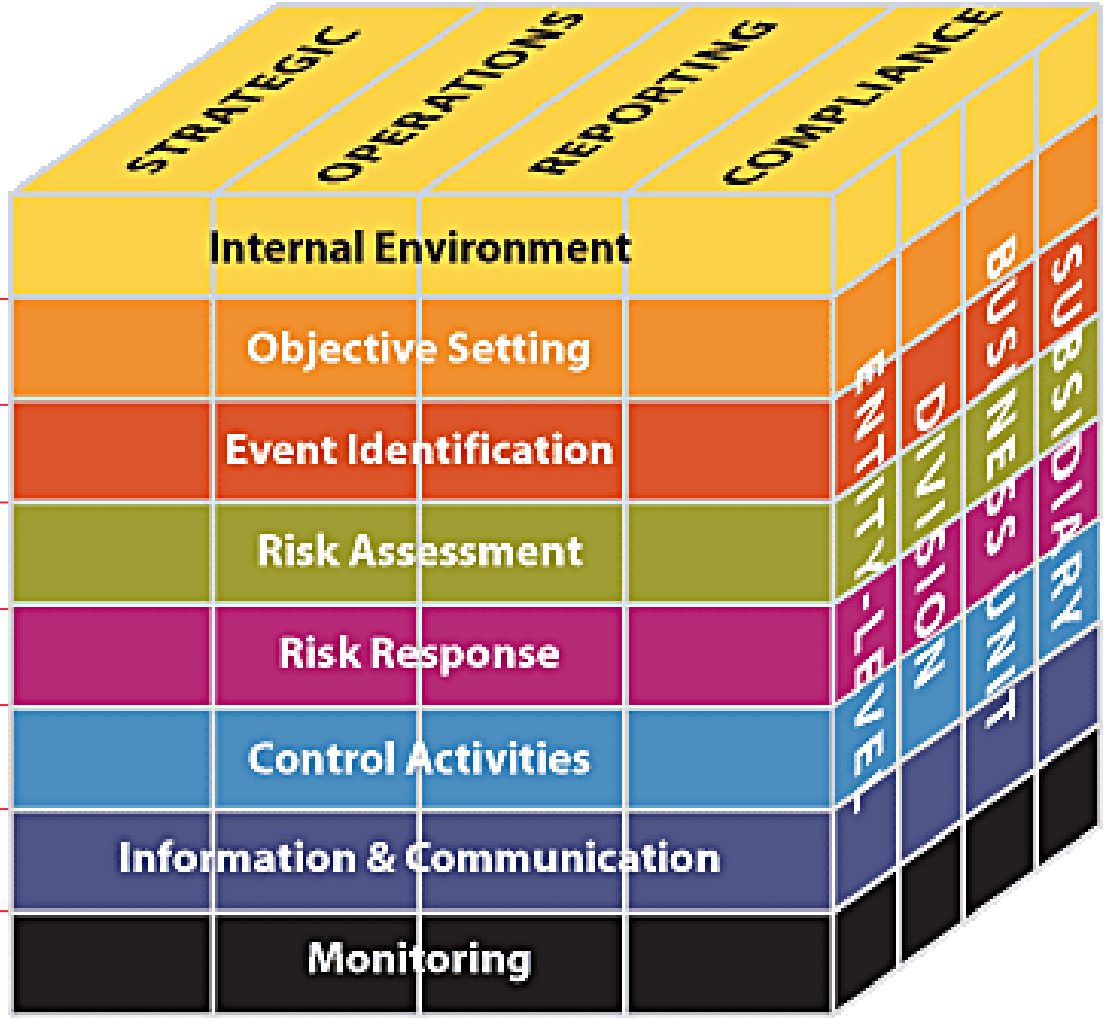
Penilaian Risiko

Perlakuan terhadap Risiko

Aktifitas Pengendalian

Sistem Informasi dan Komunikasi

Pemantauan



CRMS Indonesia (2023)

Peran IT Audit dalam Manajemen Risiko

Audit TI memiliki peran yang bergantung dan mendukung dalam manajemen risiko.

Hasil aktivitas manajemen risiko memengaruhi cara program audit TI merencanakan dan melaksanakan audit, dan temuan serta rekomendasi dari audit TI merupakan masukan penting dalam perencanaan, penilaian, dan respons risiko yang berkelanjutan.

Proses penilaian risiko dalam metodologi manajemen risiko mengidentifikasi aset dalam suatu organisasi dan mengidentifikasi serta mengevaluasi ancaman dan sumber risiko lain terhadap aset tersebut.

Organisasi dapat memilih untuk memprioritaskan audit TI menggunakan kriteria berbasis risiko yang berbeda, seperti berfokus terlebih dahulu pada proses atau komponen TI yang dinilai memiliki risiko tertinggi atau pada komponen yang dianggap memiliki nilai terbesar bagi organisasi.

Program audit TI hampir pasti beroperasi berdasarkan pendorong dan batasan lain selain panduan manajemen risiko, namun mempertimbangkan penilaian aset dan tingkat risiko membantu organisasi memastikan bahwa mereka mengalokasikan sumber daya audit TI dengan cara yang selaras dengan tujuan dan sasaran bisnis strategis.

Gantz (2014)


ANY
Questions?

3

Compliance and Certification

KEPATUHAN DAN SERTIFIKASI

Organization Must Comply (Patuh) with Regulations

Organisasi beroperasi berdasarkan berbagai aturan dan persyaratan—ada yang ditentukan sendiri, ada yang berasal dari undang-undang dan peraturan, dan ada pula yang berasal dari standar atau kriteria sertifikasi yang diikuti oleh organisasi.

Kegiatan kepatuhan mempertimbangkan semua persyaratan yang berlaku pada suatu organisasi dan menilai sejauh mana organisasi memenuhi persyaratan tersebut, mengidentifikasi kesenjangan atau kegagalan dalam memenuhi persyaratan yang mungkin ada.

Kepatuhan merupakan salah satu dimensi tata kelola yang digunakan untuk mengukur kemajuan atau kematangan organisasi dalam hal penerapan dan pelaksanaan proses dan standar tertentu secara konsisten.

Gantz (2014)

Certification for Organizations

Sertifikasi adalah jenis kepatuhan khusus. Untuk mencapai sertifikasi, Organisasi biasanya mengadopsi proses atau metodologi standar dengan cara yang ditentukan secara khusus dan kemudian kepatuhan mereka terhadap standar yang dipilih dievaluasi oleh entitas eksternal yang secara eksplisit diberi wewenang untuk memberikan sertifikasi.

Dibandingkan dengan aktivitas kepatuhan umum yang mungkin berfokus pada pendorong dan evaluasi internal atau eksternal, sertifikasi formal hampir selalu melibatkan pemeriksaan oleh pihak eksternal.

Organisasi biasanya mengetahui kriteria yang harus dipenuhi untuk mencapai sertifikasi, sehingga penilaian mandiri internal dapat digunakan untuk membantu organisasi mempersiapkan sertifikasi atau untuk memvalidasi kepatuhan berkelanjutan terhadap kriteria yang disyaratkan setelah sertifikasi.

Gantz (2014)

Types of Organizational Certifications and Standards

Certification Focus	Certifications
Quality management	• ISO 9001 • ISO 14001
Information security management	• ISO/IEC 27001 • Cybertrust
Service management	• CMMI for services • ISO/IEC 20000
Service organization controls	• SSAE 16 • ISAE 3402 • SOC 2 and 3
Process improvement	• CMMI • ISO/IEC 15504 • Six Sigma
Products or technologies	• Common criteria • CESG assisted products scheme (United Kingdom) • FIPS (United States)

Gantz (2014)

Mengelola Kepatuhan dan Sertifikasi

Mengelola kepatuhan dan sertifikasi adalah proses yang berkelanjutan, diselingi oleh tenggat waktu yang ditentukan oleh pihak eksternal atau frekuensi ujian yang diwajibkan, dalam organisasi yang tunduk pada persyaratan peraturan atau kriteria sertifikasi.

Program kepatuhan dan sertifikasi juga biasanya melakukan penilaian mandiri atau evaluasi internal yang dijadwalkan bertepatan dengan audit eksternal yang tertunda atau dilakukan secara berkala atau khusus (seperti ketika terjadi perubahan pada operasi, sistem, atau lingkungan).

Bagian dari proses pencarian dan perolehan sertifikasi adalah memastikan bahwa pengendalian, proses, atau standar yang terkait dengan sertifikasi benar-benar diterapkan di organisasi.

Gantz (2014)

Compliance and Certification Audit

Organisasi memerlukan proses internal mereka sendiri untuk menilai sertifikasi dan kepatuhan, baik mereka berharap untuk diaudit oleh pihak eksternal atau tidak, untuk membantu memastikan secara berkelanjutan bahwa mereka mematuhi persyaratan yang berlaku dan dapat menunjukkan bukti kepatuhan mereka jika dan ketika diperlukan.

Salah satu fokus sertifikasi atau audit kepatuhan yang dikelola secara eksternal adalah dengan menunjukkan secara memuaskan kepada auditor bahwa organisasi mengikuti kebijakan dan prosedurnya sendiri dan bahwa kebijakan dan prosedur tersebut diterapkan dalam praktik dan tidak hanya tertulis dalam dokumentasi resmi.

Melakukan audit internal secara teratur terhadap sejauh mana organisasi benar-benar melakukan hal-hal yang ditentukan dalam dokumentasi tersebut merupakan bagian penting dari kesiapan menghadapi audit sertifikasi eksternal dan membantu memastikan bahwa organisasi menyadari manfaat dari standar atau metodologi yang digunakan. bersertifikat.

Gantz (2014)

Peran IT Audit dalam Kepatuhan dan Sertifikasi

Peran sentral audit TI dalam kepatuhan dan sertifikasi organisasi terlihat jelas dari sifat aktivitas kepatuhan—evaluasi kepatuhan internal dan eksternal sama-sama membandingkan perilaku organisasi atau karakteristik operasional dengan serangkaian persyaratan yang eksplisit. Fitur prosedural ini merupakan ciri khas audit.

Audit kepatuhan internal mendukung fungsi pengawasan manajemen dan operasional yang dilakukan sebagai bagian dari tata kelola, sementara audit kepatuhan eksternal membantu organisasi memenuhi persyaratan hukum, peraturan, atau industri. Bahkan ketika tidak ada mandat eksternal, validasi kepatuhan dengan menggunakan audit internal memberikan informasi penting tentang banyak aspek efektivitas program atau organisasi

Gantz (2014)

Peran IT Audit dalam Kepatuhan dan Sertifikasi

Demikian pula, keberhasilan menyelesaikan **audit eksternal** sering kali menjadi prasyarat untuk mencapai atau mempertahankan sertifikasi, yang pada gilirannya memungkinkan organisasi memanfaatkan sertifikasi untuk berbagai tujuan, termasuk membedakan operasi mereka dari organisasi sejenis yang belum mendapatkan sertifikasi.

Organisasi dengan tujuan bisnis atau TI strategis yang mencakup kepatuhan terhadap persyaratan eksternal dapat menggunakan prosedur audit TI internal formal untuk mempersiapkan audit eksternal, dan mengurangi ketidakpastian mengenai hasil dan meningkatkan kemungkinan kelulusan audit tersebut.

Gantz (2014)

3

Quality Management and Assurance

MANAJEMEN KUALITAS DAN PENJAMINAN

Quality Assurance / Jaminan Kualitas

Quality assurance refers to the processes associated with achieving and maintaining a desired level of quality in a product or service.

Jaminan kualitas mengacu pada proses yang terkait dengan pencapaian dan pemeliharaan tingkat kualitas yang diinginkan dalam suatu produk atau layanan.

Gantz (2014)

Quality Assurance / Jaminan Kualitas

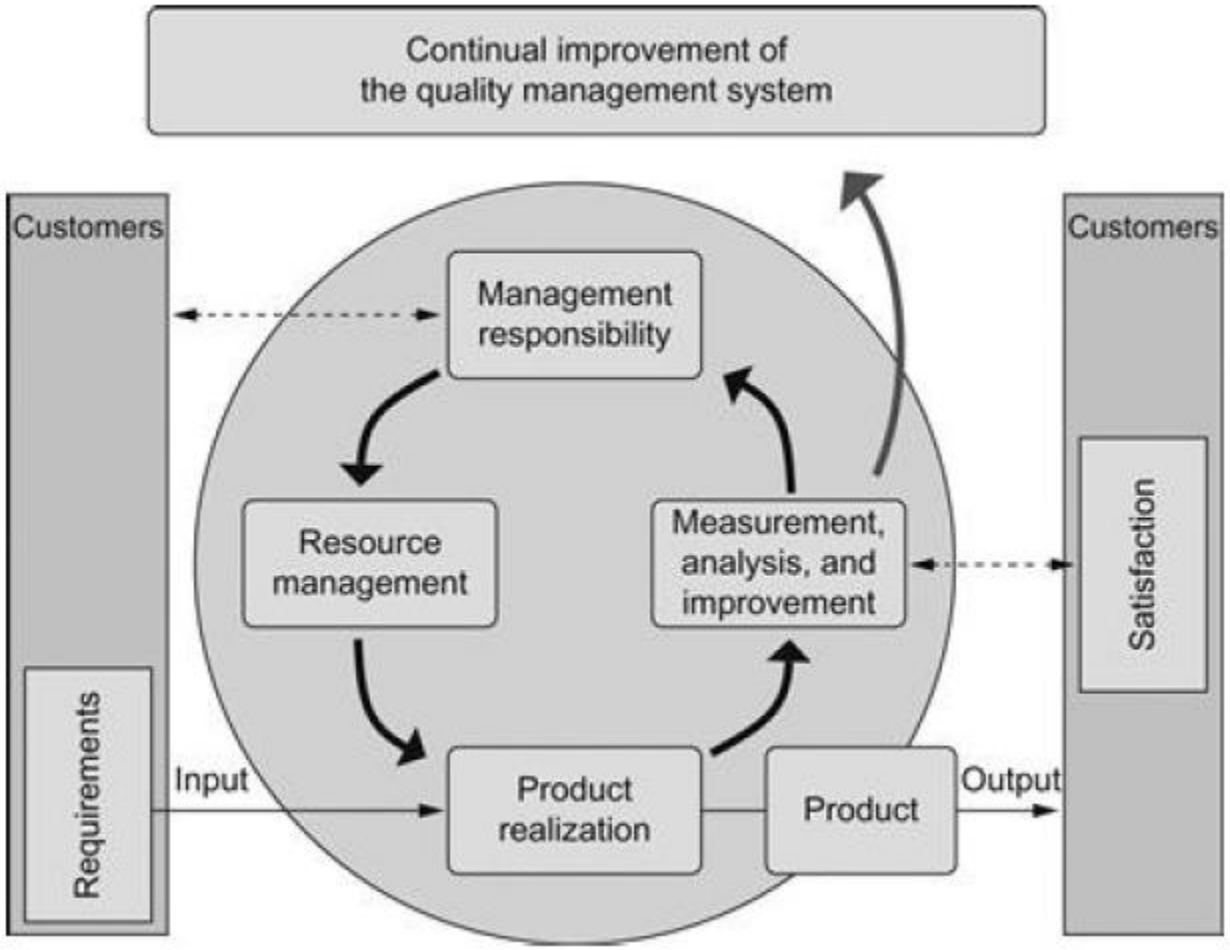
Konsep pengendalian kualitas yang berkaitan erat berfokus pada pemeliharaan kualitas yang konsisten dari waktu ke waktu, seperti memenuhi standar tertentu atau menghasilkan produk dengan karakteristik yang memenuhi kriteria yang ditentukan atau berada dalam tingkat toleransi yang ditentukan.

Istilah yang lebih umum manajemen mutu terdiri dari semua kegiatan terkoordinasi yang berkaitan dengan mutu termasuk perencanaan mutu, penjaminan mutu, pengendalian mutu, dan peningkatan mutu.

Seperti tata kelola dan manajemen risiko, metode dan praktik penjaminan mutu berlaku di berbagai tingkat organisasi. Meskipun banyak organisasi menyebutkan kualitas secara eksplisit sebagai tujuan bisnis dan mengambil keputusan untuk mengadopsi inisiatif kualitas di tingkat perusahaan, dalam praktiknya penjaminan kualitas paling sering diterapkan pada tingkat fungsi atau proses bisnis.

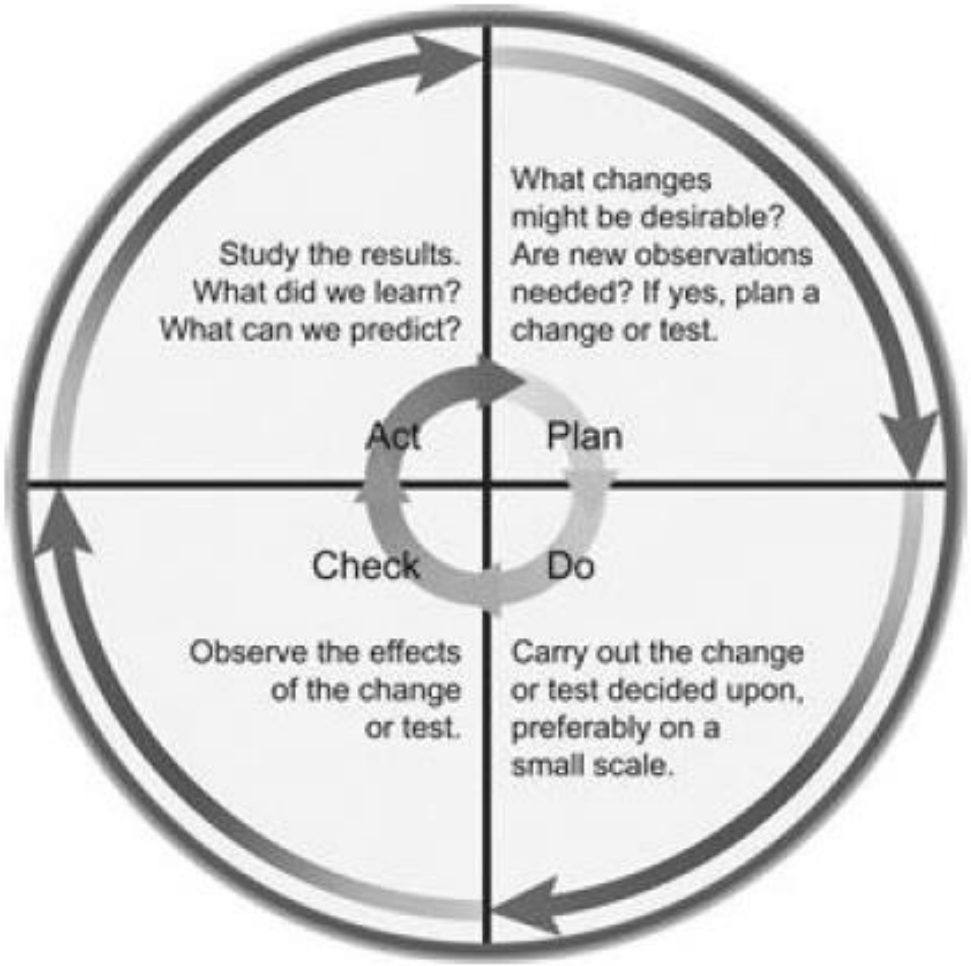
Gantz (2014)

ISO 90001 – Continuous Improvement of Quality Management System



Gantz (2014)

PDCA Cycle for Quality Assurance



Gantz (2014)

Peran IT Audit dalam Manajemen Kualitas

Audit TI mendukung fungsi manajemen mutu organisasi dengan memastikan bahwa proses operasional menghasilkan hasil yang diharapkan dan keluaran dari proses tersebut memenuhi kriteria terkait kualitas. Sistem manajemen mutu juga harus menjalani audit berkala untuk menentukan apakah sistem yang diterapkan memenuhi persyaratan yang berlaku (termasuk persyaratan yang diperlukan untuk sertifikasi) dan memenuhi persyaratan yang berlaku. dioperasikan dan dipelihara dengan baik.

Ini berarti bahwa suatu organisasi sering kali melakukan penjaminan mutu terhadap program audit internalnya (termasuk audit TI) dan melakukan audit internal terhadap sistem manajemen mutu dan proses terkait. Beberapa jenis audit TI dapat digunakan dalam aktivitas manajemen mutu atau penjaminan mutu, termasuk audit produk atau layanan, proses, atau sistem kontrol terkait Teknologi Informasi.

Gantz (2014)

4

Information Security Management

MANAJEMEN KEAMANAN INFORMASI

Information Security

Information Security

Penekanan saat ini dalam manajemen keamanan informasi pada pemantauan berkelanjutan, penilaian ancaman dan kerentanan, serta evaluasi penerapan dan efektivitas pengendalian keamanan tumpang tindih dengan praktik audit TI sedemikian rupa sehingga keamanan informasi memerlukan pertimbangan terpisah.

Kontrol keamanan—administratif, teknis, dan fisik—adalah fokus utama manajemen keamanan informasi dan aktivitas audit atau penilaian TI yang dilakukan untuk mendukung program keamanan informasi.

Manajemen keamanan informasi mencakup pemilihan, implementasi, konfigurasi, operasi, dan pemantauan kontrol keamanan yang memadai untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan data yang dikandungnya.

Gantz (2014)

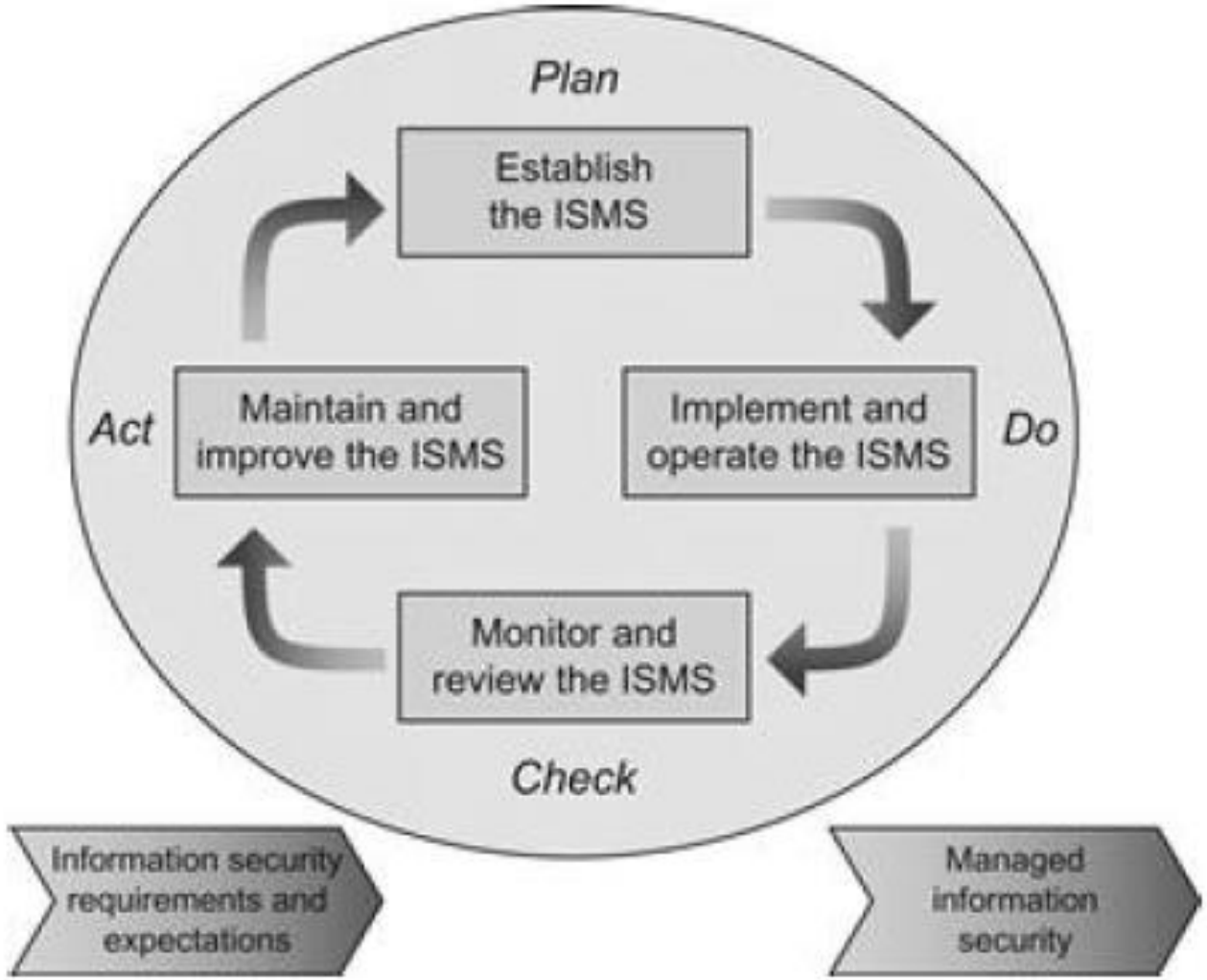
Information Security Berbasis Risiko

Manajemen keamanan informasi adalah berbasis risiko, dalam arti bahwa keputusan untuk menerapkan mekanisme keamanan atau mengalokasikan sumber daya untuk melindungi aset organisasi harus menyeimbangkan biaya penyediaan keamanan dengan tingkat risiko terhadap organisasi, jika ancaman yang dihadapi tetap tidak diatasi.

Dalam istilah ekonomi sederhana, tidak masuk akal bagi suatu organisasi untuk berinvestasi lebih banyak pada keamanan daripada nilai aset yang dilindungi atau besarnya atau kerugian yang akan terjadi jika aset tersebut hilang, dicuri, dirusak, atau dirusak.

Gantz (2014)

ISMS Process defined in ISO 27001 applies PDCA Model to Information Security Management



Gantz (2014)

Peran IT Audit dalam Manajemen Keamanan Informasi

Manajemen keamanan informasi mendukung audit TI dengan mengambil tanggung jawab untuk menerapkan dan mengonfigurasi kontrol internal terkait keamanan dengan benar.

Pengendalian keamanan merupakan subjek penting dari pengendalian internal, namun masih merupakan bagian, yang berarti keamanan informasi tidak mencakup seluruh pengendalian TI dalam suatu organisasi.

Audit TI juga mendukung manajemen keamanan informasi, dengan memberikan pemeriksaan rinci dan kritis terhadap pengendalian internal yang diterapkan untuk mencapai tujuan keamanan dan dengan memastikan bahwa operasi TI sesuai dengan kebijakan, prosedur, standar, dan pedoman organisasi.

Gantz (2014)

Referensi

Angel R. Otero (2019). Information Technology and Control (Fifth Edition). Taylor & Francis.

Sanyoto Gondodiyoto (2007). Audit Sistem Informasi Pendekatan CobIT. Mitra Wacana Media.

Stephen D. Gantz (2014). The Basics of IT Audit. Syngress, Elsevier.

CRMS Indonesia (2023). Qualified Risk Management Professiona. LSP MKS.

Penugasan Terstruktur

Tugas Individu 1

Mencari contoh studi kasus penggunaan salah satu dari berbagai framework tata Kelola TI yang digunakan oleh sebuah organisasi.

Jelaskan dalam bentuk essai yang berisikan perusahaan, framwork yang digunakan, dan alasan menggunakannya.

Tata laksana menjawab :

Ketik dalam format A4 1.5 space.

Kumpulkan di Elitag.

Deadline : Minggu ke-7 pukul 09.00

Penugasan Terstruktur

Tugas Kelompok 1

Penentuan Studi Kasus Kelompok :

Kelompok 1 – SIAKAD

Kelompok 2 – Sistem PMB

Kelompok 3 – SIM Praktikum

Kelompok 4 – SIMKP

Kelompok 5 – ELITAG

Kelompok 6 – SIM Point

Kelompok 7 – Sistem Perpustakaan

Kelompok 8 – JConnect

Tugas :

Membuat daftar 10 risiko teknologi informasi pada studi kasus yang diberikan.

Urutkan risiko berdasarkan tingkat keparahannya (low, moderate, high)

Gunakan berbagai referensi eksternal untuk membuat identifikasi risiko (termasuk materi kelas RPPL)

Tata laksana menjawab :

Ketik dalam format A4 1.5 space.

Kumpulkan di Elitag.

Deadline : Minggu ke-7 pukul 09.00

Kegiatan Mandiri

Mempelajari secara mandiri mengenai Prosedur Audit Teknologi Informasi